REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	7 June 1996	Master's Thesis, 2 Aug 95 - 7 Jun 96

4. TITLE AND SUBTITLE
The Operational Denial of Commercial Space Imagery

5. FUNDING NUMBERS

6. AUTHOR(S)
Major Anthony J. Russo, U.S. Air Force

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, Kansas 66027-1352

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 words)*

This study investigates the capability of the United States to deny commercial space-based imagery to its adversaries during times of hostilities. The United States recognizes that this imagery poses a threat to national security interests, but has not identified a mechanism for operational denial of this information. In 1994 the Clinton Administration removed the U.S. ban on the export of high-resolution imagery because the proliferation of space-based sensors makes this information commonly available whether or not it is the Untied States that sells the imagery. This study examines U.S. space policy, domestic and international space law, and previously suggested approaches to countering the threat posed by this imagery. The study also examines technical feasibility as well as operational effectiveness of 28 proposed solutions. The conclusion of this study is that the United States does not currently have a system or methodology for denying space-based imagery in all cases. However, three different types of laser systems could be developed into a potentially effective countermeasure to space-based imagery. These systems include a high-powered ground-based laser, a high-powered airborne laser, or mobile, low-powered lasers that could function as tactical jammers of space-based senors.

14. SUBJECT TERMS
Commercial Satellite Imagery

15. NUMBER OF PAGES

16. PRICE CODE
98

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unlimited

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to ***stay within the lines*** to meet ***optical scanning requirements***.

Block 1. Agency Use Only *(Leave blank)*.

Block 2. Report Date. Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least the year.

Block 3. Type of Report and Dates Covered. State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

Block 4. Title and Subtitle. A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

Block 5. Funding Numbers. To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

C	- Contract	**PR**	- Project
G	- Grant	**TA**	- Task
PE	- Program Element	**WU**	- Work Unit Accession No.

Block 6. Author(s). Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

Block 7. Performing Organization Name(s) and Address(es). Self-explanatory.

Block 8. Performing Organization Report Number. Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es). Self-explanatory.

Block 10. Sponsoring/Monitoring Agency Report Number. *(If known)*

Block 11. Supplementary Notes. Enter information not included elsewhere such as: Prepared in cooperation with...; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

Block 12a. Distribution/Availability Statement. Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

- **DOD** - See DoDD 5230.24, "Distribution Statements on Technical Documents."
- **DOE** - See authorities.
- **NASA** - See Handbook NHB 2200.2.
- **NTIS** - Leave blank.

Block 12b. Distribution Code.

- **DOD** - Leave blank.
- **DOE** - Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.
- **NASA** - Leave blank.
- **NTIS** - Leave blank.

Block 13. Abstract. Include a brief *(Maximum 200 words)* factual summary of the most significant information contained in the report.

Block 14. Subject Terms. Keywords or phrases identifying major subjects in the report.

Block 15. Number of Pages. Enter the total number of pages.

Block 16. Price Code. Enter appropriate price code *(NTIS only)*.

Blocks 17. - 19. Security Classifications. Self-explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

Block 20. Limitation of Abstract. This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

*U.S.GPO:1993-0-358-779

THE OPERATIONAL DENIAL OF COMMERCIAL SPACE IMAGERY

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE

by

ANTHONY J. RUSSO, MAJ, USAF
B.S., Lehigh University, Bethlehem, Pennsylvania, 1982
M.S., Air Force Institute of Technology, Wright-Patterson AFB, 1987

Fort Leavenworth, Kansas
1996

THE OPERATIONAL DENIAL OF COMMERCIAL SPACE IMAGERY

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE

by

ANTHONY J. RUSSO. MAJ. USAF
B.S., Lehigh University. Bethlehem. Pennsylvania. 1982
M.S., Air Force Institute of Technology. Wright-Patterson AFB. 1987

Fort Leavenworth. Kansas
1996

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Anthony J. Russo

Thesis Title: The Operational Denial of Commercial Space Imagery

Approved by:

_____, Thesis Committee Chairman
LTC Deborah D. Gregoire, M.B.A.

_____, Member
Vicky LH Scherberger, Ph.D.

_____, Member, Consulting Faculty
LTC James C. McNaughton, Ph.D.

Accepted this 7th day of June 1996 by:

_____, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (Reference to this study should include the foregoing statement.)

ABSTRACT

THE OPERATIONAL DENIAL OF COMMERCIAL SPACE IMAGERY by MAJ Anthony J. Russo, USAF, 98 pages

This study investigates the capability of the United States to deny commercial space-based imagery to its adversaries during times of hostilities. The United States recognizes that this imagery poses a threat to national security interests, but has not identified a mechanism for operational denial of this information. In 1994 the Clinton Administration removed the U.S. ban on the export of high-resolution imagery because the proliferation of space-based sensors makes this information commonly available whether or not it is the United States that sells the imagery.

This study examines U.S. space policy, domestic and international space law, and previously suggested approaches to countering the threat posed by this imagery. The study also examines technical feasibility as well as operational effectiveness of 28 proposed solutions.

The conclusion of this study is that the United States does not currently have a system or methodology for denying space-based imagery in all cases. However, three different types of laser systems could be developed into a potentially effective countermeasure to space-based imagery. These systems include a high-powered ground-based laser, a high-powered airborne laser, or mobile, low-powered lasers that could function as tactical jammers of space-based sensors.

TABLE OF CONTENTS

LIST OF ILLUSTRATION

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Problem Statement

The importance of surprise in all levels of military operations has been recognized since at least the time of Sun Tzu. High-resolution satellite imagery is now commercially available from a number of sources and threatens the ability of the U.S. to achieve surprise against potential adversaries. Technology has advanced to the point where militarily significant intelligence can be provided, realtime, to anyone with a credit card. A March 1994 decision by the Clinton Administration now allows U.S. companies to sell one-meter resolution satellite images outside the U.S. This change in policy simply acknowledges the fact that this unprecedented quality imagery will soon be widely available whether or not it is the United States that builds and orbits the satellites. The proliferation of this technology threatens the ability of the U.S. to achieve dominance in Information Warfare. Dr. William Perry, the Secretary of Defense, acquiesced to lifting of the export ban on this kind of intelligence data, but with the caveat that he "needed a way to turn off the spigot" during times of crisis.[1] Can the United States deny the use of commercial imagery to adversaries during times of hostilities?

Background

On the 24th of February 1991, in what he described as a "Hail Mary play," General H. Norman Schwarzkopf, Commander of U.S. Central Command (CENTCOM), boldly maneuvered around the left flank of the entrenched Iraqi divisions in the Kuwaiti Theater of Operations

(KTO). At a press conference later that day, General Schwarzkopf acknowledged that he did not initiate this risky "Hail Mary" maneuver until he was sure that he had taken out all of the Iraqi reconnaissance assets.[2] At 0732 (local time), a commercial French satellite, *Satellite pour l'observation de la terra* (SPOT) *III*, was overhead in the KTO and took medium-resolution photographs of the beginning of this flanking maneuver.

While executing this maneuver, CENTCOM's forces were lined up nose-to-tail along the only east-west road in this sector, and highly vulnerable to Iraqi attack. Fortunately, France was an active member of the coalition against Iraq and exerts a large degree of control over its commercial assets. The intelligence data was collected and processed, but not passed to Iraq. Coalition forces appear to have achieved tactical surprise and friendly casualties were extraordinarily light.[3] If the Iraqi forces knew that the coalition forces were making the "Hail Mary" maneuver, could they have done anything about it? No one knows whether or not the specific outcome would have changed, but it is known with certainty that the CENTCOM commander felt it was important enough to wait until the Iraqis were completely blinded before he made his move.

On 24 July 1990, only a few days before Iraq invaded Kuwait, U.S. industry leaders in remote sensing from space testified before Congress on the need to lift the ban on exporting satellite imagery and related products. These industry leaders were supported by several academic sponsors and political allies but were strongly opposed by the Department of Defense (DoD). The industry leaders were not successful; the export ban remained in place.[4]

In late 1992, the issue was again raised before Congress and again was defeated by DoD objections. However, by February 1994, U.S. commercial interests successfully lobbied their Congressmen to lift the ban. They argued, correctly, that keeping the ban would not stop the proliferation of high-resolution imagery, it would only mean that U.S. companies would not be

the ones selling it.[5] The Russians, desperate for hard currency, were already selling two-meter resolution photos from one of their military spy satellites and made a big marketing hit by highlighting very detailed photos of sensitive U.S. installations.[6] Japanese and European companies were making great strides in remote sensing technologies, and the number of commercial applications was greatly expanding. Given these conditions, it would have been pointless to prevent U.S. companies from competing in this lucrative arena. Dr. Perry, who would later be confirmed as Secretary of Defense, reluctantly agreed to allow the production and sale outside the U.S. of one-meter resolution photographs. However, Dr. Perry still recognized that these commercial products could and would have serious military applications that threaten U.S. strategic interests. The Department of Defense briefed Congress on the need to prevent these products from entering the hands of an adversary but did not offer a specific solution.[7]

Operational Definitions and Key Terms

The following list of definitions provides the working vocabulary for a discussion of denial of space-based imagery.[8] A more comprehensive discussion of the terms is included in the Glossary.

ASAT. An antisatellite weapon. Any system designed to destroy satellites. For purposes of this thesis, use is limited to so called "hard-kill" systems where permanent loss of utility is inflicted on a particular asset. However, this term will be used broadly enough to encompass different technologies that achieve this result.

Bandwidth. The width of a given frequency band in Hertz. The bandwidth is determined by subtracting the lowest frequency in the operating spectrum from the highest. In general, an asset with greater bandwidth has greater capacity. Transmitters cannot pass certain types of information if the bandwidth is too narrow.

Bus. Everything on a satellite except the payload(s). The bus includes the structural frame, power, attitude control, thermal management systems and tracking, telemetry and control subsystems. The bus supports the payload, but the payload performs the mission of the satellite.

Constellation. A system of like satellites. Constellations are usually designed to provided increased coverage and redundancy for essential mission functions.

Control Segment. One of three components of any space system. The control segment provides for stationkeeping, orbital changes, attitude and stabilization changes, and other general maintenance activities.

Crosslink. A satellite-to-satellite communications link. Crosslinks allow control of a satellite not in view of a control segment.

Directed Energy. Concentrated energy in a tight beam, like a laser.

Geostationary Orbit. A satellite that has a period of one day and orbits the equator. To a ground-based observer, the satellite will appear to remain in the same fixed location in the sky.

Low Earth Orbit (LEO). A satellite rapidly orbiting the Earth at a low altitude (approximately 200-1500 kilometers (km)) is said to be in LEO. Almost all satellite imagery is collected by satellites in LEO.

Multispectral. A means of subdividing the spectrum into smaller bandwidths. Adding or subtracting these subdivisions can be useful in terrain or target analysis.

Particle Beam. Streams of subatomic particles that are accelerated to high fractions of the speed of light and formed into a tight beam that does not diverge.

Payload. The portion of a satellite that performs the satellite's primary mission. A payload must be supported by a bus. There can be multiple payloads on a satellite.

Space Segment. One of three components of any space system. The space segment is the portion that is physically in space.

Tracking, Telemetry and Control (TTC). Electronic remote monitoring of a satellite's functions and position in space. Used by the control segment to maintain or adjust the space segment.

Terminal Segment. The last of the three components of any space system. The Terminal segment receives space-based data, either unprocessed or processed.

Limitations

Much of the literature on this topic is founded on an outdated view of the world. The denial of space-based information has invariably centered on a hypothetical U.S. vs. Soviet Union space war. Since the Soviet Union no longer exists, this body of research will have to be interpreted in the context of the current world geopolitical situation. While much of the available literature concerns a potential strategic nuclear war, this thesis is focused on the lesser, but more likely threat of some belligerent using a third party commercial source for intelligence data useful in a military operation. The third party could be completely innocent in this arrangement and might even be partially or wholly owned by U.S. corporations. Since this particular aspect of the space negation problem has not been discussed in the literature, this thesis extrapolates from the proposed anti-Soviet ASATs that are well documented.

This thesis relies on purely unclassified sources. Since there may be significant bodies of research that are classified, this thesis is limited to only a portion of the total community body of knowledge. However, since this thesis is focused only on feasibility, all of the technical details are not necessarily relevant to the conclusions.

Delimitations

This thesis is limited to commercial space-based imagery. Other types of space-based information may also be a significant threat to U.S. interests, but will not be addressed in this

thesis. Some of the results of this thesis may be partially or wholly applicable to other types of space systems. For example, an examination of a potential adversary's use of commercial communications satellites or the free access to precise navigation signals from Global Positioning System (GPS) could produce similar concerns. A similar thought process could be used to assess potential countermeasures to address these concerns. However, a specific solution recommended by this thesis might not be relevant to a different type of system.

Thesis Question

Can the United States deny the use of commercial imagery to adversaries during times of hostilities? The growing trend in information systems, particularly space-based information systems is away from a monolithic structure operated by a single country. The new trend is towards a proliferation of special purpose commercial systems that are not indigenous to any one country's military machine. For example, International Maritime Satellite Corporation (INMARSAT) is a multinational commercial entity that operates a constellation of communications satellites. There are currently 92 member nations, including such diverse countries as the United States, United Kingdom, China, Syria, and Iran. More importantly the rapidly expanding number of services available through this constellation can be purchased by *anyone*, not just member nations. The potential list of customers includes rogue nations, narcotraffickers, terrorist groups, or even private individuals. U.S. ASAT debates have usually postulated developing a system to destroy some specific space asset, usually some asset associated with the Soviet Union--which no longer exists. This "hard-kill" approach may not be feasible or appropriate against a threat from assets owned by U.S. corporations or its allies.

Subordinate Question

Does the U.S. possess the technical means to deny information from commercial space assets to potential adversaries? While each space system has some unique technical characteristics, some are common to all systems. For example, every photoreconnaissance system must:

1. Collect the raw data. This collection is called "imaging." It requires that some type of sensor be physically placed over the geographic area of interest. Typically this is done by placing a satellite in a "low Earth orbit," or LEO, so that it rapidly circles the Earth and arrives at different places at different times. This orbit permits coverage of most of the Earth's surface at a distance that allows high resolution images.

2. Transmit the data. The satellite must then have some means of sending the data to a processing station on the ground. In the past, this could have meant the need to de-orbit a film canister which would have to be physically picked up and delivered. However, this procedure is now considered primitive by today's standards. Computer and communications technology has advanced to the point where satellites can transmit this data electronically to the ground station.

3. Process the data. Next the raw data must be converted into a usable product for sale. Modern systems collect so much raw data that some screening must be done to determine which piece is really information as opposed to just data.

4. Disseminate the product to the customer. Finally, the information product must reach the customer who, for purposes of this thesis, will be considered a potential adversary.

In order to deny the potential adversary this threatening information, the United States must interdict some portion of this cycle. This thesis will examine a number of ideas suggested in the literature for technical feasibility in accomplishing this task

Subordinate Question

Can the United States devise a system to operationally deny adversaries access to high resolution images from space? The U.S. might conceivably have the technical means to deny information to an adversary, but this technical solution might not be feasible operationally. For example, if the U.S. possesses the means to interdict satellite imaging from one satellite sensor. but the adversary has access to multiple sensors on different platforms, then the U.S. does not have an operationally feasible solution to the problem. Alternately, the U.S. could possess the technical means to deny imaging over the United States, but lack the ability to deploy this technical means to the geographic area where it is conducting operations. This. too, would be an operationally ineffective solution.

Subordinate Question

Can the United States devise a system to operationally deny access to high resolution space imagery that is consistent with existing U.S. and international laws? It is conceivable that the United States could deploy an operationally effective system that has the technical ability to interdict some portion of the imaging cycle described but be unable to legally employ that system. This thesis will examine the constraints posed by current U.S. law and relevant international agreements concerning operations in space. This thesis will also make an assessment as to which of the technical solutions suggested in the literature seem consistent with these laws and agreements.

Subordinate Question

Can the United States devise a system to operationally deny access to high resolution space imagery that is politically acceptable? It is conceivable that a proposed technical solution might be operationally effective and legally defensible and still not be employed due to political

considerations. More precisely, the administration might view a negative public perception associated with certain solutions as not worth the military gain. While what is or is not politically acceptable is obviously highly subjective, this thesis will address this issue in terms of historical precedents. This thesis will also discuss the issue in terms of the current public debate and the implications of that debate on potential solutions to the problem defined.

Underlying Assumptions

1. The United States needs the capability to operationally deny commercial satellite imagery.

2. The United States will not deploy a system that violates U.S. or international law, or that abrogates an international treaty that the United States has signed and that the Senate has ratified, or that is politically unacceptable.

3. The thesis and its conclusions will be based entirely on unclassified sources, but the implementation of any given solution might be covert or unacknowledged.

Significance

Sun Tzu recognized that "all warfare is based on deception"[9] and spoke extensively about feints, secret agents, and surprise attacks. The winning commander will always be the one that correctly assesses the situation and attacks the enemy when he least expects it. Clausewitz also recognized this principle and described the fog of war that makes the simple things in war difficult. Obviously a successful commander will seek information that reduces this fog and will simultaneously do anything he can to decrease the amount of accurate information available to the enemy.

Current Army doctrine recognizes surprise as one of the ageless Principles of War, with intelligence itself considered a Battlefield Operating System. Fires are governed by the "decide-

detect-deliver-assess" cycle where reconnaissance assets clearly are needed to perform the Detect and Assess phases in the cycle. The U.S. Army divides the battlefield in five complementary elements. One entire element is devoted to security and reconnaissance, specifically focused on preventing the enemy from obtaining information about its main forces.[10] Air Force doctrine also recognizes these principles and Air Force Manual (AFM) 1-1, Basic Aerospace Doctrine of the U.S. Air Force, discusses the Observe-Orient-Decide-Act (OODA) loop theory governing combat. The theory suggests that the side that can perform the functions of this loop the quickest will be the victor.[11]

The ability of the United States to achieve surprise at the strategic, operational, or tactical level is now threatened by the information explosion. Comprehensive information about virtually any topic is widely available from multiple sources. The quality, accuracy, and quantity of the information are unprecedented. The Services recognize that the world is in an Information Revolution analogous to the Industrial Revolution that led to American preeminence in the world. The military's ability to support Unites States national interests will depend on its ability to win the Information War. A proposed draft to AFM 1-1 goes as far as to rank "Counter-Information" as a mission area coequal to "Counter-Air"--traditionally the Air Force's first priority in any conflict.[12]

CHAPTER 2

LITERATURE REVIEW

On 9 February 1994, the House of Representatives opened a joint hearing of the Science, Space, and Technology Committee and the Permanent Select Committee on Intelligence concerning the commercialization of space imagery. The two House committees heard lengthy testimony from a wide variety of speakers representing the Central Intelligence Agency (CIA). DoD, State Department, and Commerce. The DoD opposed the lifting of the U.S. export ban on high resolution satellite imagery because of national security issues.[1]

The committees also heard from a panel of Chief Executive Officers (CEOs) and chairmen of the board from various companies involved in remote sensing. These industry leaders presented evidence that the types of imagery DoD was concerned about were already on the market. Congressman Brown chairman of the joint session displayed a two-meter resolution photograph of the U.S. Capitol taken by a Russian satellite. The photograph had been sold commercially. The industry leaders predicted that the customer base for this type of imagery would be $15 billion by the year 2000. They also argued for unrestricted licensing to compete in this lucrative market and to sell these images without government control. They claimed that an open U.S. policy would actually enhance national security as U.S. companies would secure a larger market share and be more willing to voluntarily restrict access to imagery during times of national crisis. They specifically argued against the DoD proposed restriction of "shutter control," which would allow the Defense Department to shut off the collection of any images it deemed counter to the national interest. The industry leaders expressed the opinion that this would make

U.S. companies unreliable suppliers of imagery to its customers and would place an administrative cost on the collection system that would render it noncompetitive in an international marketplace.[2]

Congress sided with industry and the DoD currently has no independent authority to restrict access to high-resolution imagery sold by licensed U.S. companies. The first of these new generation of photo-reconnaissance systems will be launched by 1997. By the Year 2000. thousands of images will be available each day from a variety of commercial sources.[3] The military implications of the availability of this information are profound. Table 1 provides a brief survey of some of the types of features that can be discerned at various spatial resolutions.[4]

TABLE 1

GROUND RESOLUTION REQUIREMENTS FOR OBJECT IDENTIFICATION
(in meters)

Target	Detection	General ID	Precise ID
Bridges	6.0	4.5	1.5
Troop Units	6.0	2.0	1.2
Aircraft	4.5	1.5	1.0
C2 Headquarters	3.0	1.5	0.6
Surface Ships	7.5	4.5	0.6
Vehicles	1.5	0.6	0.3
Surfaced Subs	30.0	6.0	1.5
Roads	7.5	6.0	1.8
Terrain		90.0	4.5

Source: James G. Lee, "Counterspace Operations for Information Dominance," (Thesis, Maxwell Air Force Base, AL: School of Advanced Airpower Studies, October 1994), 15.

Table 1 demonstrates the potential use of commercial satellites for the collection of military intelligence by quantitatively describing the physical performance needed. Other researchers have noted that even relatively primitive commercial imaging satellites have significant military utility. For example, the first purely commercial satellite the French *Satellite pour l'observation de la terre* (SPOT) has only a 10-meter resolution, yet SPOT Image Corporation openly advertises the military advantage it provides customers.[5] SPOT imagery was used by Iraq to plan its invasion of Kuwait, and it was used by the United States throughout DESERT SHIELD/DESERT STORM. Although the SPOT Image Corporation keeps its client list confidential, one author estimates that as much as 80 percent of their business is meeting military customer's needs. By far, their largest customer, overall, is the U.S. military.[6] SPOT Imagery can be obtained directly by some subscriber nations through their own ground stations, or images can be distributed electronically to customers who do not have their own ground station. Some SPOT images are even available on the Internet.

Although SPOT is the most visible example of a commercial system that has the potential to be a military threat to U.S. interests, it is by no means the only commercial system available. Russia has been energetically attempting to gain market share and earn hard currency by commercially selling images from its military satellites. Japan has a more primitive version of SPOT in orbit now, but launches a new satellite next year that will be capable of collecting one-meter resolution images. Other nations are scrambling to get a foothold in this growth industry. In his recent Naval War College thesis, Commander Donald Meyer describes the current imaging systems available to third parties and discusses the threat to U.S. national security.[7] Similarly, Lawrence Hunt and Jeffrey Miller describe current systems, innovative emerging technologies and defense implications of the proliferation of commercial systems.[8] Air Force Major Edwin

Swedberg also provides a survey of current and planned commercial systems and focuses on the effect this would have on operational and tactical surprise for U.S. military forces.[9]

U.S. Policy on Countering Commercial Imaging Satellites

When the Russians launched Sputnik 1 on 4 October 1957, the United States government made a conscious decision not to object to the overflight of its sovereign territory by the spacecraft. This established a precedent that space is international territory, analogous to the oceans, and that all nations have the right of free passage. The exact definition of where a nation's airspace ends and where international "space" begins remains an unanswered legal question, but the principle of freedom of access to space is a consistent principle of U.S. Space Policy.[10]

With the launch of Sputnik, the U.S. military rapidly accelerated its satellite program and began to explore methods of satellite negation. The purpose of this exploration was to find ways to counter the expected use of Soviet space capability to conduct military reconnaissance. During the late 1950s and 1960s the U.S. military devoted significant efforts towards its satellite reconnaissance program to enhance national security, while publicly avoiding the issue. U.S. Policy secretly acknowledged that satellite reconnaissance was provocative at best, and might potentially be considered illegal in the international arena.[11]

In 1975, President Ford signed National Security Decision Memorandum (NSDM) 345 directing the Department of Defense to develop an operational AntiSatellite (ASAT) system. The purpose of this program was to negate Soviet reconnaissance satellites in LEOs and to provide deterrence against the use of Soviet ASATs against our own reconnaissance satellites.[12]

The Carter Administration openly acknowledged the "fact of" U.S. space reconnaissance capabilities--which was already in the public domain despite years of official denials. President Carter also acknowledged that the United States was conducting research on ASATs, which he said the U.S. needed to deter the Soviet Union in the absence of specific arms control agreements

restricting their use. In 1978, President Carter signed Presidential Directive (PD) 37 which indicated a shift in emphasis from purely civilian applications of space capabilities towards capabilities that enhanced national security. The signing of a very comprehensive PD-37 acknowledged publicly that space was a warfighting medium essential to our national survival and that Soviet space systems posed a threat to our national security.[13]

President Reagan signed a National Security Decision Directive (NSDD) which superseded all previous presidential space policy directives. NSDD-42, signed in 1982, established the U.S. position--held to this day--that "peaceful purposes" in the exploitation of space means "nonaggressive" and not "nonmilitary." A nation that conducts activities in space in pursuit of national security goals has not violated the peaceful purposes clause. The directive acknowledged that space systems are national property and that interference with objects in space constituted an infringement of a nation's sovereign rights. However, it also stated the U.S. would "pursue activities in space in support of the United States inherent right of self-defense."[14] NSDD-42 also called for development of an operational ASAT system to protect U.S. security interests.

President Reagan also signed NSDD-85 which indicated the U.S. would be willing to base weapons in space with the purpose of negating the Soviet threat of Inter-Continental Ballistic Missiles (ICBMs). He later updated and reissued his national space policy in NSDD-293 which called for a robust and comprehensive ASAT capability at the earliest possible date. This was reinforced by National Security Directive (NSD) 30, which was signed the following year by President Bush. These documents acknowledged a commercial sector for the first time, but were still focused on the Soviet Union as the principal threat.[15]

The collapse of the Soviet Union caused the U.S. military to look seriously at Rest-of-World (ROW) space systems. As a result, the services submitted a proposed revision to the DoD

Space Policy in 1992. This draft policy addressed the threat to U.S. national security posed by non-Russian military, civil and commercial space systems. As of this writing, a new Space Policy has not been signed and NSD-30 remains the official U.S. Policy. However, during DESERT STORM the activities and statements of the United States established policy precedent for future operations. During that conflict, the U.S. State Department brought diplomatic pressure on France to halt the sale of commercial satellite images from SPOT to Iraq. According to an Air Force space lawyer:

> The declared intent and publicly declared right was to deny, degrade, and disrupt space operations related to adversaries' warfighting capacity during conflict. There was actual interruption of remote sensing imaging in the theater of operations.[16]

The proliferation of space-based imagery drives a clear requirement for methods of denying this information to an adversary.[17] Each of the Services has developed doctrine to implement NSD-30. For example, the Air Force Space Operations Doctrine calls for a Joint Force Commander (JFC) to rapidly acquire space superiority in a conflict by employing forces to "deny enemy access to space information."[18] Similarly the new Army Field Manual 100-6, Information Operations, calls for the JFC to interdict space-derived information and even addresses the issue of dealing with the commercial sources of this information. In essence, it suggests that certain U.S. and allied companies would be willing to voluntarily restrict access or even sabotage their own systems, if they could be assured plausible deniability.[19]

Legal Implications on Countering Commercial Satellite Imagery

The first restriction on the use of space is found in the Limited Test Ban Treaty of 1963. This international law specifically banned nuclear tests or other nuclear explosions in space, regardless of the purpose of the explosion.[20] In 1967, the United Nations (UN) codified the basic principles of space law into a kind of "Magna Carta" document for space that is commonly referred to as the "Outer Space Treaty." This document remains the foundation of all current

space law, although there are significantly different interpretations of some of its provisions. Article I of the Treaty established the right of all nations to explore and use outer space. Article II prohibits the appropriation of space, in the name of sovereignty, by any country.[21]

Article III of the treaty applies all international law, including the entire Charter of the United Nations, to the use of outer space. This is highly relevant to the issue of one nation's right to deny another's use of satellite imagery. Several authors argue that since international law prohibits acts of aggression and the threat or use of force, any action that interferes with a nations space system must be prohibited by Article III's broad inclusion of the United Nations Charter.[22] Since Article 51 of the UN Charter gives all nations the right of self-defense, other authors express the opinion that attacks on a nation's reconnaissance system would be an acceptable response to an armed attack. However, by that line of reasoning:

> even though the article [UN Article 51] allows a response to an armed attack, it does not allow attacks against spacecraft of states that are not part of the armed conflict. Further, that author argues that the article does not permit an attack on a satellite when that attack coincides with the beginning of the hostilities.[23]

The United States does not share the above interpretation. The U.S. has argued that, in light of the lethality of the modern battlefield, the right of self-defense includes even pre-emptive military action in cases where there is a presumed threat of attack.[24] The United States subscribes to the view determined at the international military tribunal at Nuremberg that military necessity permits a nation:

> subject to the laws of war, to apply any amount and kind of force to compel the complete submission of the enemy with the least possible expenditure of time, life, and money . . . . There must be some reasonable connection between the destruction of property and the overcoming of the enemy.[25]

Obviously this force must be applied to a military target, but dual-use objects are also permissible targets if the military advantage gained outweighs the damage to the civilian sector. For example,

bridges and power plants in Iraq were destroyed despite civilian casualties and disruption to legitimate commercial activity.

Article IV of the Outer Space Treaty is also controversial. One author goes as far as to blatantly state that "Article IV prohibits military activity in space."[26] However, this is an extreme interpretation as the actual wording of the Treaty merely prohibits weapons of mass destruction from being placed in orbit and reserves the Moon and "other celestial bodies" for exclusively "peaceful purposes." Since the preamble also mentions the term "peaceful purposes," many authors have interpreted that phrase to apply to all space activity and not just those on the Moon. The real controversy concerns the definition of "peaceful." The United States maintains that "peaceful" could apply to all military activity taken against Iraq in accordance with the UN Resolution authorizing the use of force.[27] However, the body of literature suggests that the U.S. is virtually alone in that interpretation. For example, Bin Cheng writes in the Journal of Space Law:

> flying in the face of the international acceptance of the word "peaceful" as evidenced by the nuclear energy treaties, the Antarctic Treaty and in fact the clear wording of the Outer Space Treaty itself, the United States insists that "peaceful" in Article IV, paragraph 2 means not "non-military," but "non-aggressive." The simple fact that the United States' interpretation has the effect of making the first sentence of Article IV, paragraph 2 . . . meaningless and redundant shows that it cannot be correct. The Soviet Union opposes it. Friends and allies of the United States--some having been bullied or duped into accepting the United States' interpretation--mostly suffer in silence, sorrow and despair.[28]

Despite the hand-wringing over the word, military activity in space started with the first launch of a space object and will continue indefinitely. Many nations currently operate military or civil/military systems including Russia, China, Israel, France, Brazil, India, Italy, Germany, and the Arab League.[29] A number of other nations are on the threshold of having their own space capability; one study estimates that 729 new payloads will be launched in the next five years.[30] Well over one hundred nations buy space services from corporations like SPOT Image, INMARSAT, or INTELSAT and apply these services to military purposes. While one can argue

that "peaceful" really meant "non-military" in Article IV of the Outer Space Treaty, it is not credible to argue that only the United States uses space for military purposes.

The last Article of the Outer Space Treaty that is relevant to the discussion of denial of commercial satellite imagery is Article VI. Article VI requires that states "bear international responsibility for national activities in outer space . . . whether such activities are carried on by governmental agencies or nongovernmental entities."[31] Once again the interpretation of this stipulation is controversial as the term "national activities" is vague, but the U.S. interprets this to mean that nations are responsible, and therefore liable, for misuse of space by their commercial sector.[32] Therefore, by extension, if a corporation sold Iraq imagery in defiance of a UN ban on trade with Iraq, then that corporation's nation could be held financially liable for this violation. Interpreted this way, the U.S. could, theoretically, exert diplomatic leverage to help control a commercial entity in another country.

Although the Outer Space Treaty of 1967 is the most significant document in the establishment of space law, other treaties and agreements that are relevant to commercial satellite imagery have been signed by the United States. In 1972, the U.S. and U.S.S.R signed the Anti-Ballistic Missile (ABM) Treaty. This treaty prohibited the development, test or deployment of ABM systems or their components. Strictly interpreted, this language could hinder the development of some potential technical solutions to the problem of denial of satellite imagery, since it could be argued that systems or components might also have a role in countering ballistic missiles or the other side's reconnaissance satellites (also forbidden in the treaty). In 1985, the United States rejected this restrictive interpretation and took the position that development and testing of nonfixed ABM missiles and systems that operate under "other physical principles" is not restricted by the ABM Treaty.[33] The United States has continued to move away from the strict

wording of that treaty since 1985. One of the reasons for the recent partial government shutdown is a dispute over congressional language that would essentially abrogate this treaty entirely.

The Convention on International Liability for Damage Caused by Space Objects is another multilateral treaty that bears examination. The treaty, signed in 1973, holds nations responsible for damage caused by one of their space objects. There is no distinction between military or civilian space objects. In terms of hostilities, however, this treaty would be suspended between the belligerents and would not restrict actions between them. The status of third parties supporting one of the sides is not addressed in this treaty.[34]

In 1980 the Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques was signed. This treaty prohibits the employment of any modification of the environment that has a widespread, long-lasting or severe effect on the environment. The treaty applies to outer space as well as to the terrestrial environment. The treaty prohibits actual employment only. Research, development, and test are not restricted.[35]

As early as 1970 the United Nations recognized that satellite imagery caused unique legal concerns, even in the specialized field of space law, and tasked the United Nations Committee on Peaceful Uses of Outer Space (COPUOS) Legal Subcommittee to address this issue. After fifteen years of debate, mostly over differences with U.S. interpretations of space law, the COPUOS drafted the "Principles Relating to Remote Sensing of the Earth from Space," where remote sensing is defined as "the sensing of the earth's surface from space through the detection and gathering of electromagnetic waves emitted, reflected, or defracted by objects."[36] These Principles were passed in 1986 by the General Assembly of the United Nations as UN Resolution 41/65. Unlike the multilateral treaties, this UN Resolution is not binding on the member nations, but does form a basis for customary international law, to the extent that they become part of accepted practices.[37]

The Principles are significant in their expression of remote sensing activities as being conducted for the benefit of all nations. The "sensing" state must notify the "sensed" states and provide access to the collected data "on a nondiscriminatory basis and at a reasonable cost."[38] The Principles also hold nations responsible for remote sensing activities of nongovernmental entities operating from their country.[39] Thus, a third party operating a satellite has legal responsibilities for the data it collects and provides to one belligerent about another belligerent.

In addition to international law, the discussion of solutions to the problem of denial of commercial satellite imagery is constrained by U.S. domestic laws. For example, Title 18, U.S. Code Section 1367 specifically prohibits the interference with any satellite transmission. Commonly referred to as the "Captain Midnight" Law, this legislation was passed in 1986 to establish criminal penalties for the malicious mischief conducted by an individual that took over an HBO broadcast. It was not intended to restrict legitimate government activities as evidenced by a specific exemption made for law enforcement and intelligence activities. United States Space Command (USSPACECOM) and its components do not fit the definition of exempted agencies, but clearly Congress did not intend to apply this law to the exercise of space control to enhance national security. Although this law should not be considered a serious impediment to those solutions that rely on interference of a commercial satellite transmission, the matter is serious enough that it would require the DoD to seek a clarification from the Attorney General prior to actual employment of any system.[40]

Although the Captain Midnight Law was not an attempt to constrain space control efforts, Congress has, occasionally, attempted to restrict the development of ASATs. In this context, ASATs are usually defined as weapons that cause permanent destruction to a satellite. During the 1980s Congress did pass Public Laws 98-94 and 98-473 which limited the number of tests of the F-15-launched ASAT and required the administration to try to negotiate an ASAT ban with the

Soviet Union. Subsequent appropriation bills further restricted testing of specific ASAT systems and deleted funding for the Army and Air Force ASAT programs.[41]

These bills stopped short of prohibiting these programs, and the language was specific to the systems currently in work. However, the Services naturally became reluctant to risk scarce funding dollars on programs that kept being reduced by Congress, and the ASAT programs of the 1980s withered and died. Two specific attempts to ban ASATs, in 1981 and 1983, were not successful--largely due to strong opposition in the Executive Branch.[42] Since that time, the make-up of Congress has dramatically changed--to the point that Congress now proposes deploying a space-based weapon system to defend against ballistic missiles.

Operational Denial of Commercial Imagery Systems
Possible Solutions

Perhaps the easiest and least provocative potential solution to the problem posed by commercial satellites is passive countermeasures which require no new technology development or acquisition of equipment. Swedberg argues that passive countermeasures can be effective in some scenarios to deny an adversary access to critical information about U.S. forces. He describes passive countermeasures as restricting operations to times when the threat satellite is not overhead or when it cannot image effectively due to environmental conditions (night, cloud cover, etc.). When it is not possible to remain out of view of a threat satellite, Swedberg advocates the use of cover, concealment, or deception practices to retain the element of operational and tactical surprise. Swedberg acknowledges that passive countermeasures would not be sufficient in certain scenarios. For example, the buildup of ground forces in preparation for the invasion of Iraq would not have been a good candidate for this approach.[43]

Another approach is to ask for the voluntary cooperation of the satellite operator. During the 1994 Joint Congressional Hearing that led to the lifting of the commercial imaging restrictions

in the United States, corporate leaders expressed a willingness to not pass data that compromised national security. This might be effective in situations where the threat satellite was owned by a U.S. corporation and the threat to national security was obvious. However, the industry leaders were reluctant to allow DoD to be the judge of what constituted a national security concern for fear that DoD would invoke the phrase over trivial issues and decrease the reliability of U.S. firms.[44] Certain non-U.S. corporations might also voluntarily comply with U.S. desires to restrict access at times given the clear international law on the restriction of space to peaceful purposes. However, the presumption is that they would be less willing to risk market share to support U.S. national interests than a U.S. company.

A slightly more heavy-handed approach would be to simply ban the transmission of satellite imagery from U.S. corporations. This would require a Presidential order, but there are precedents that allow for restrictions on commercial activity during times of national crisis. The President could also indirectly influence foreign corporations through diplomatic pressure on the host nation. Since the host nation is responsible for the misuse of space by its commercial entities, this can be an effective lever. This approach was advocated by numerous authors and is codified in Air Force Space Operations Doctrine.[45] As previously mentioned, a form of diplomatic pressure on France resulted in cutting Iraq off from SPOT imagery during DESERT STORM. The term "diplomatic pressure" applies to a spectrum of activity ranging from a polite request--to enticements or deals--to threats or coercion. Economic pressure could be brought to bear by suing under the Liability Convention or through traditional boycotts, reductions in foreign aid, etc.[46]

A December 1995 Defense News analysis of the Army's new field manual on information operations suggested another possible avenue to deny accurate satellite imagery to U.S. adversaries. The analysis suggested the U.S. firms would be willing, provided they were ensured

plausible deniability, to assist the U.S. military in deceiving or disrupting information services to U.S. adversaries. The article cited routine instances of corporate cooperation with the National Security Agency as precedent for this type of activity.[47] This type of extraordinary support from U.S. corporations would probably have to be arranged on a case-by-case basis. This type of "self-sabotage" opens up a number of legal issues that have not yet been addressed by any of the international or domestic laws discussed in this thesis.

The preceding nonmaterial solutions focus on preventing commercial enterprises from sending processed information to a U.S. adversary. Another approach to the problem would be to prevent the commercial entity from collecting the threatening data in the first place. One obvious way to accomplish this is to attack the collection asset directly. The United States has already demonstrated that this can be done. On 15 September 1985, the United States successfully tested an ASAT against a discarded Solrad satellite. The technique is called "direct ascent" and consists of a F-15 launching a Short-Range Attack Missile (SRAM) containing a Miniature Homing Vehicle (MRV). The MRV does not carry a warhead, but can destroy its target satellite with kinetic energy since it travels at over 13 km per second. The MRV is self-guided with an infra-red detection system. The F-15 MRV program was canceled in 1988, largely due to a lack of Congressional support.[48]

The Russians have also extensively tested kinetic energy ASATs and are believed to have an operational ASAT that works on a slightly different principle. The Russians use a co-orbital interception of the target, which is less reliable than the U.S. approach, but far less complicated and much cheaper. Their interceptor is launched on a SL-11 ICBM and achieves a co-planar orbit with its intended target.[49] The interceptor then maneuvers to its target using an active radar signal and explodes within 1-9 km of its target. One or more of the many metal shards then impacts the target satellite. According to the United Nations Institute for Disarmament Research, the former

Soviet Union has tested this system at least 20 times since 1968 and is highly confident in its operational effectiveness.[50]

Other types of kinetic energy ASATs are discussed in a 1990 RAND report on ASAT arms control. One of the key findings was that virtually any ABM could also serve as de facto ASAT. In 1989 the U.S. Army took the lead in the acquisition of a ground-based interceptor which would have a dual role against ballistic missiles or low-orbiting satellites. The program, Exoatmospheric Reentry Interceptor System (ERIS), was a ground-based missile that was self-guided to its target. The program was canceled in 1991 after getting poor support from Congress. The Navy also had a short-lived program based on a sea-launched Tomahawk missile. Another concept relies on advanced placement of small interceptors in LEO. The interceptors lie dormant until a crisis erupts and are then launched against selected targets, destroying them with the kinetic energy of impact. These interceptors were called "Brilliant Pebbles" when they were part of the Strategic Defense Initiative (SDI), but are generally referred to as "space mines" in the context of counter space.[51] In fact, *any* space object that can maneuver could be employed as a *de facto* space mine. For example, a U.S. satellite that has had its payload fail while in orbit might use its remaining fuel to maneuver into the orbit of a target satellite. The interception would be a complicated task and would not work for all sets of possible orbits, but might be more politically acceptable than deploying dedicated space weapons.

A classified MITRE Corporation study on high-altitude ASAT weapons suggests several hard-kill approaches that do not rely on the kinetic energy of an actual space collision. One unclassified approach the study discusses in detail is the use of nuclear radiation against satellites. In a modern nuclear explosion 80 percent of the energy is released in the form of X-rays. In the atmosphere this energy is absorbed and converted into blast and thermal energy. This is the primary source of the destructiveness of a nuclear weapon. However, in space the energy is not

absorbed, but propagates freely until it strikes some object. The radiated power is decreased by the square of the distance, but only a tiny fraction of the original energy is needed to create havoc with sensitive satellite electronics. In addition, the outer skin of the satellite will absorb the incident X-ray energy. This causes shock damage resulting in permanent destruction of the satellite's payload without actually shattering the satellite as was the case with a kinetic energy impact.[52]

Since the blast is not directional, all satellites within a given region of space will be affected. The nuclear blast will affect an even larger volume by charging the molecules in the atmosphere in a process known as "scintillation." Scintillation will disrupt satellite communications through that volume of space. Another effect from the nuclear burst is Electromagnetic Pulse (EMP). EMP is caused by currents generated by emitted gamma rays that then interact with matter in the atmosphere. This effect generates freely propagating high frequency radiation that can affect satellites at over 1000 km from the point of the blast. The exact effects of EMP on a satellite are still not understood, but satellites are generally considered an exceptionally soft target with respect to electromagnetic effects.[53]

The Russians were aware of the inherent ASAT capability of their nuclear-tipped Galosh missiles since they deployed them as an ABM weapon in 1962.[54] It is a reasonable assumption that this was also a key reason for the United States' desire to prohibit nuclear explosions in space when they signed the Limited Test Ban Treaty in 1963. Based on what is known about the physical phenomena of a nuclear explosion in space, any ballistic missile carrying a nuclear warhead is an effective, albeit non-discriminatory, means of denying satellite imagery in a selected region of space. However, fratricide to U.S. satellites and collateral damage to third parties would be an unavoidable by-product of such an approach. During the SDI program, there was considerable speculation about the feasibility of a space-based x-ray laser that would get around

this problem. The concept was to combine the directionality of a laser with the destructiveness of x-rays. A small, controlled nuclear explosion would be used to power the laser that would be directed at the target with minimal fratricide and collateral damage. However, this part of the SDI program was deleted prior to development.[55]

Another major class of ASAT weapons discussed in relevant literature is Directed Energy Weapons (DEWs). General Piotrowski, then USSPACECOM commander, said that the Russians already had a high-powered ground-based laser with operational capability to destroy satellites in LEO and potentially interfere with those in high and elliptical orbits.[56] Ironically, the existence of this laser at Sary Shagan test range was made public after being located with a commercial satellite imager, SPOT.

The Sary Shagan laser is estimated to be in the 1 to 3 megawatt range and capable of destroying a satellite out to 400 km. However, it can achieve a "soft-kill" by overheating key satellite components at up to 1200 km.[57] The latter range would encompass all commercial imaging systems of any military significance. Of particular advantage to this approach is the fact that--done judiciously--this soft kill attack may not be attributed to a hostile action. For example, gradual reduction of a satellite`s solar cells will slowly kill it by depriving it of its power source. This type of effect can closely resemble the failure of a satellite due to "natural causes," and might therefore allow the attacking nation plausible deniability. Another potential weak point on an imaging satellite would be the imaging sensor itself. Since, by its very nature, the sensor is highly sensitive to a certain part of the electromagnetic spectrum (usually visible light or Infrared), an intense source of energy "in-band" could destroy the sensor while leaving the rest of the satellite undamaged.

Since 1988, the United States Army as had an experimental ground-based laser at White Sands, New Mexico. The 2.2 Megawatt (Mw) chemical laser, called MIRACL, is only in the

Research and Development (R&D) stage, but has an inherent capability to interfere with imaging satellites in LEO. Although the laser is not powerful enough to destroy a satellite, it could interfere with various components which might temporarily disrupt its operation or potentially lead to its destruction. One possible scenario:

> Several aggressive moves in the course of successive orbits, at a level of power far below lethal dose, would after all damage the attitude and observation control sensors, the solar cells, the telecommunications or remote control receivers and the electronic equipment on board the satellite, which if attacked in this way would rapidly expire from this "galloping senility."[58]

Although not mentioned in the above scenario, it should be possible to selectively choose components that do not necessarily result in the destruction of the satellite. For example, if only the attitude control sensor was disrupted, it might be possible for the satellite's owner to correct this problem on a subsequent orbit and reorient the satellite. This would have the effect of causing the satellite to miss a key collection point, without inflicting any permanent damage. To date, Congress has not allowed the Army to test the MIRACL laser against an object in space.

Another potential basing mode for directed energy weapons would be to place them in space. During the SDI program, researchers investigated the possibility of using space-based lasers fueled by chemical interaction. A hydrogen-fluoride (HF) laser was thought to be the best candidate at the time this portion of the program was canceled. An HF laser, mounted on a satellite, would have the advantage of unrestricted line of fire and would be free from the difficult problem of propagating through the atmosphere. The technological leap required to acquire, track and hit a satellite would be considerable easier than hitting a Theater Ballistic Missile (TBM) a few seconds after it clears the clouds.[59]

Another concept, again developed in response to the TBM threat, would be to mount a chemical laser on an airborne platform. The Air Force has completed concept definition of an Airborne Laser (ABL) and is seeking funding to develop operational prototypes. The ABL is a modified Boeing 747 that carries a 2 Mw Chemical-Oxygen-Iodine Laser (COIL). The COIL is

also powered by chemical interaction and would be capable of firing many times before needing to be refueled. The ABL is being designed to counter TBMs, not to perform counterspace missions, but once again the technology required to acquire, track and hit a satellite would be significantly easier than hitting a TBM. The ABL is designed to destroy a TBM in a few seconds with 95 percent confidence out to a range of 250 km.[60]

Although this range is insufficient to destroy most commercial satellites, the previous discussion of potential satellite weak points is even more applicable here. Unlike ground or even space-based lasers, the ABL would have extreme flexibility in the timing of its attack. Therefore, less-than-lethal disrupting attacks would have more significance, since they can be timed so that they will deny imagery at the crucial moment. The ABL flies at an operational altitude of 45,000 feet.[61] The laser will not have to contend with clouds, but will still have to propagate through the atmosphere. However, recent advances in adaptive optics allow for correction for losses normally associated with atmospheric distortion. This means that the laser will reach its target with minimal loss of power due to the atmosphere. The limiting factor, as with all directed energy techniques, would be the reduction of power due to distance.

Most of the literature concerning directed energy weapons has focused on high-powered lasers that are designed to destroy their targets. The previous discussion illustrates how these "hard-kill" systems might have counterspace applications beyond their lethal range. However, another approach might be to design a directed energy system that has absolutely no destructive power at all. Phillips Lab has sponsored experiments that indicated even low-power commercial lasers can be effective at temporarily jamming optical sensors. This effect occurs at power levels far below what would be required to damage satellite components at typical satellite altitudes. Preliminary evidence indicates that low-power laser jamming may be effective even when the

laser is "out-of-band" to the target--making detection, and therefore attribution, difficult. According to one proposal:

> A laser produced spark within a sensor produces copious in-band radiation [even if the laser is out-of-band] . . . . Moreover, the copious spark radiation that is produced . . . opens the possibility for a laser jammer that works against a wide variety of sensor platforms.[62]

The authors of this proposal discuss primarily antimissile applications, but the earlier discussion indicates that this phenomena would be effective against satellites as well. As the optics in commercial sensors improve, this effect becomes even more pronounced, since a sensor that is more sensitive to a certain band of the spectrum will also process more of the generated "noise." This concept allows rapid deployment of small, lightweight laser jammers on ships, aircraft, or mobile vans that have the capacity to momentarily blind a sensor when it is in position to see something the United States does not want it to see.

The term "directed energy" applies to more than just lasers. Lasers are commonly discussed because their properties are well understood, but satellites can be attacked by weapons that operate in other parts of the spectrum as well. The most commonly referred to alternative to lasers is high-powered microwaves. According to James Hackett and Robin Ranger, the former Soviet Union has already demonstrated a laboratory model capable of putting out billion watt pulses.[63] If this number is accurate, then it is feasible to develop a weapon that could interfere with on-board electronics of any satellite in LEO, possibly causing subsystem failures. According to James Lee:

> Intelligence estimates suggest it is possible to construct a microwave radiation weapon today with a satellite soft-kill capability of 500 km. In addition, microwave radiation at lower power levels can effectively be used for satellite jamming.[64]

Despite these claims, and unlike the literature on lasers, there is no quantitative data published to support the feasibility of building a high-powered microwave weapon or to predict just how effective it would be. It is known that the Russians have made an extensive investment in this

technology, so it is a reasonable assumption that their experiments have found reason to continue this line of research.

Directed energy weapons and kinetic impact weapons are similar in the respect in that they both target the satellite that is the collection point for data the U.S. consider a threat. Another approach to counter this threat is to target the links between the satellite and the ground segment. All satellites need to communicate with the controllers on the ground to conduct basic stationkeeping activities, receive their collection taskings and to report back with the information collected. Just as the United States practiced electronic warfare in DESERT STORM to disrupt Iraqi communications, it can conduct electronic warfare to disrupt either the uplink or downlink of a satellite to prevent the passing of threatening data. There are two principle methods of accomplishing this, jamming and spoofing.

Jamming involves transmitting on the same frequency band as either the telemetry link between the satellite and its ground segment or the link between the terminal segment and the satellite.[65] Usually the jamming signal is transmitted at a higher power than the legitimate signal and induces an increase in the bit error rate until either the satellite or the ground station loses lock.[66] This has the effect of preventing communication between part of the legitimate owner's system, but the effect only lasts while the jammer is on and in the coverage footprint of the satellite. The power required to jam leaves an electronic signature which may prevent plausible deniability. On some satellites, the collected data can be stored and downlinked at another control station further along its orbital path. Therefore multiple jammers are needed in diverse geographical regions. Some satellites, particularly older imaging satellites, either do not have sufficient on-board storage or do not have many ground stations to transmit to. Jamming is more effective against these kinds of systems.

The French Institute for International Relations cites anonymous sources in its report to the UN to allege that the United States already possesses this capability mounted on its aircraft carriers.[67] While this allegation is unconfirmed in the literature and highly suspect, jamming orbital assets is a recognized part of Air Force doctrine.[68] Jamming has obvious advantages as a space control measure as it is relatively easy to do and delays information from falling into adversary hands without damaging the space asset.

Spoofing, the other type of electronic warfare, requires greater sophistication. Spoofing is a deceptive measure where the United States would assume the role of an authorized user by sending a legitimate command to the satellite at the right frequency and in accordance with all the protocols the satellite expects.[69] If the satellite can be made to accept the unauthorized commands instead of its legitimate owner, then there is a wide range of possible events that the U.S. could initiate. For example, the United States could have the satellite erase its memory right after it collected imagery the U.S. did not want it to pass, or the U.S. could have it turn itself off for an orbit or two. Although usually considered a nondestructive attack, spoofing can have destructive effects. For example, the satellite could be ordered to de-orbit or to consume all its fuel in a maneuver that puts it hopelessly in the wrong orbit. Spoofing requires detailed intelligence on the satellite's command protocols, but has the potential to be one the most subtle methods to deny threat information to an adversary.

Rather than trying to interdict the link between the space segment and either the control segment or the terminal segment, an alternate approach would be to directly attack the ground station. This is particularly attractive when it is possible to identify the location of an adversary's receipt of satellite imagery. This site can then be attacked by special operations forces or precision air strikes to cut off the supply of information. This approach was put in practice when Iraqi satellite receivers were knocked out early in DESERT STORM.[70]

Many nations currently collect commercial imagery at their own dedicated ground sites, so this approach has some merit. However, the recent trend is towards small, mobile terminals and information passed over computer modems. Attacking the nation's indigenous ground stations would have little effect if some other third party government or commercial entity was still willing to pass them the information and they had the means to receive it. This has led some authors to suggest that the best approach to ensure this information does not reach the adversary, is to practice active Information Warfare (IW). While all of the proposed solutions discussed thus far have been a form of IW, the term often refers to new techniques involving computer viruses, logic bombs, disruption of telecommunications, and the implanting of false data.[71]

The specific target could be anyone of the links in the imagery process, but the commercial entity's central processing facility would probably be the most effective location for an IW attack. An effective IW attack requires detailed intelligence about the information being collected and the mechanism for processing and transferring the information. It would also require an extraordinary degree of access to that commercial entity's information processing network. Provided these conditions are met, IW provides enormous flexibility to deny or alter information an adversary receives about U.S. forces.

As the commercial imaging satellites become more and more sophisticated, their precise position in space becomes increasingly important to their collection of high resolution imagery. According to Laslo Szentpeteri's report for the Foreign Aerospace Science and Technology Center, "It is only possible to utilize the capabilities provided by the increasingly improved optical devices if we know the exact spatial position and orbit of the remote sensing device."[72] Szentpeteri's report has absolutely nothing to do with counterspace operations, but this single line from his report suggests a future vulnerability of sophisticated imaging systems. Many satellite operators may turn to Global Positioning System (GPS) for precise navigation signals because the

service is free and GPS receivers are commonly and inexpensively available. Those that turn to GPS will realize a performance edge over those that do not.

However, as sole owner of the GPS, the United States could intentionally degrade the accuracy of the signal at a critical time. Alternately, the U.S. could selectively jam or spoof the receiver on the particular satellite of interest, as GPS signals are one of the easiest to override. Either approach, especially if done unexpectedly, would have the effect of seriously degrading the satellite's imaging performance. While this would deny key information to an adversary at a critical time, the effect on the third party satellite would be temporary and nondestructive.

Summary of the Literature

The proliferation of commercial imaging satellites has been noted by many authors, and many have suggested that the United States needs a capability to counter these satellites. Official U.S. policy has also been clear on the need for solutions to this problem, although Congress has acted to restrict the testing of destructive ASATs against actual space targets in the past. As a result of the Cold War, most of the research--and therefore the literature--that discusses counterspace, does so in the context of a space war between superpowers. The emphasis is on permanent destruction of the space segment through ASATs. However, many of the Cold War ASAT concepts and the emerging anti-TBM concepts have less-than-lethal modes that may be more useful in countering third party systems. Since a satellite in LEO is a far easier target than a TBM, the technological leap is far smaller.

The review of the literature has also suggested alternatives to attacking the space segment. As the information is collected, processed, and disseminated, there are several places where the United States could act to interdict this information and prevent its eventual transmission to an adversary. Some of these proposed solutions do not rely on developing new technology.

The legal constraints of a U.S. response to a commercial threat are complex, as the interpretation of space law varies substantially between the U.S. and most other nations. While very little is strictly forbidden in specific terms, the broader interpretations generally applied in many countries would make virtually any U.S. action illegal if it involved a third party to a conflict. The United States, however, maintains that the United Nations charter has clearly recognized a nation's inherent right to self-defense and this certainly applies to the space medium as well.

CHAPTER 3

RESEARCH METHODOLOGY

The design of the research methodology focuses on the primary question: Can the United States deny the use of commercial imagery to adversaries during times of hostilities? The literature review has shown conclusively that the proliferation of commercial satellite imagery raises national security issues and that the United States has a need to deny adversaries access to this imagery during certain times.

The literature relating to commercial satellite imagery suggests potential solutions to the problem. Although there is substantial overlap among the various authors discussing commercial satellite imagery, the review of the literature identified 28 distinct potential solutions relevant to the primary research question. These potential solutions, contained in 15 different primary sources, were not necessarily advocated by the authors of the source articles. Some of the authors discussed potential measures to deny satellite imagery as a means of outlawing such activity. The criteria for inclusion of a potential solution in this analysis are: (1) the idea is a credible method of denying an adversary access to commercial satellite imagery; (2) the idea has either been published or was part of a government-sponsored research effort; and (3) the idea is sufficiently distinct from other potential solutions to merit individual discussion.

In order to classify the various potential solutions to the research problem, it is useful to think of the collection of imagery as a system supported by multiple interdependent subsystems. To successfully interdict the flow of information to the adversary, the United States must enter the imaging process at some point and disrupt at least one of these subsystems. The designs of

imaging systems vary and therefore the capabilities, limitations, and vulnerabilities of these systems will also vary. However, all imaging systems are governed by the same laws of physics. Common aspects, generic to any imaging system, do not vary significantly with the individual system design.

Therefore the research methodology will analyze each of the 28 different potential solutions according to the phase of the imagery process that it affects. The solution will be evaluated by four primary criteria that are derived from the secondary research question. Each of these primary criterion will be given a numerical score based on the answers to specific tertiary questions defined in this chapter. The results of these numerical ratings will then be displayed in a Decision Matrix according to the format described in U.S. Army Command and General Staff College Student Text 25-1.[1] A notional display of this format is shown on Table 2.

TABLE 2

EXAMPLE OF DECISION MATRIX

SOLUTION	TECHNICAL	OPERATIONAL	LEGAL	POLITICAL
SOLUTION 1	4	4	2	3
SOLUTION 2	3	3	3	3
SOLUTION 3	4	1	3	4
SOLUTION 4	2	4	3	4
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
SOLUTION 28	4	4	4	1

Major Imagery Subsystems

As mentioned in Chapter 1, every satellite, regardless of design, has to collect, transmit, process, and disseminate data to the end user. The United States can act at any one of those points to achieve the desired result.

Collection. In order for data to threaten U.S. interests, some asset must collect the data. While this is a rather obvious statement, this simple fact opens up multiple approaches to defeat satellite imagery by taking advantage of the known physical constraints involved in collecting this imagery. To begin with one could expect that any commercial satellite collecting high resolution images will be in LEO. Conceivably, other orbits could work, but a LEO is most economical and will therefore be used by any *commercial* entity.

A satellite in LEO will orbit at an altitude between 200 and 1500 kilometers. Commercial satellites will most likely orbit at the middle of the range due to problems with longevity and maintenance of the orbit at lower altitudes and loss of resolution at higher altitudes. Low altitude translates into a rapid orbital period. A typical satellite might orbit the Earth every 90 minutes, and, because of the rotation of the Earth, the satellite's ground trace will vary on each pass. This means, that for any given geographic area of interest, a single satellite will only be in view for a few minutes on a given pass. It may not have a favorable pass over that particular spot again for several days to several weeks.

Another constraint on the collection subsystem is the fact that in order for a satellite to "see" something, it must first "look." In other words, to produce an optical-quality photograph a satellite must have a sensor that operates in the visible light portion of the electromagnetic spectrum. This is a relatively narrow band that has its own limitations. For example, Swedberg suggested that the United States could maintain operational and tactical surprise by conducting operations at night.[2] Some commercial sensors do use portions of the spectrum other than visible

(such as infrared), and, in general, the spectral range of the sensor is usually limited to whatever is suitable for the particular commercial application it was designed to fulfill. During hostilities, adversaries will attempt to apply existing commercial sensors to military purposes, just as the United States used commercial LANDSAT imagery during DESERT STORM to help make tactical maps. However, these satellites are not specifically designed for military operations, which creates limitations the U.S. can exploit.

Some examples of solutions that interdict the imaging process at the collection point are: cover, concealment and deception (CCD) activities, operational constraints (such as only moving at night), and ASATs.

Transmission. Data collected by a satellite cannot threaten U.S. interests unless it can be sent to a ground station for processing. The United States is unique in that it has a comprehensive worldwide network of ground stations for TTC (Tracking, Telemetry and Control) of its satellites. The United States maintains constant communication with its satellites as they continually traverse the Earth. This makes good sense for military assets, but is hardly cost effective for a commercial enterprise. Commercial applications can usually wait for a satellite to swing back into view to download collected data. Therefore they usually have only a few, and sometimes only one, ground station(s) capable of accepting the data from the satellite.

These data are collected at one time and place and are transferred to Earth at another. In general, the United States will know the time and place that this transfer is likely to take place. Temporarily disrupting this link can delay the transmission of the data for several hours. In some cases, the satellite might not have sufficient storage and the data might be overwritten by subsequent collections.

An example of a technical solution that interdicts the transmission link of the imaging cycle is the downlink jammer discussed in Lee's thesis on counterspace dominance.[3]

Processing. Not all data collected by commercial satellites is useful, and even useful data will not necessarily threaten U.S. security interests. To threaten U.S. interests, some commercial entity must process the raw data and convert it into a useful information product. This will most likely be done at a single, central processing facility. This part of the imaging cycle will likely require a highly technical work force and a lot of automation support. Potential solutions interdict the cycle at this point could deny or delay information to the adversary, or perhaps deceive them by altering the information before it is passed. Examples of this type of interdiction would be various types of Information Warfare, such as logic bombs or malicious code.[4]

Dissemination. The dissemination subsystem is the portion that actually provides the information to the U.S. adversary. Commercial satellites could collect, transmit and process all the data in the world without threatening U.S. interests if the information were not obtained by a hostile party. The processed information product is the real threat--provided the commercial entity that prepared it can transfer it to our adversary. Currently, a likely adversary would have limited technical means to receive the information electronically. However, in the near future, this kind of information will be readily passed over the Internet. "Demo" images from the French commercial satellite SPOT can already be accessed over the Internet, and it is just a matter of time before any individual can order satellite images the way some people electronically purchase retail items.[5]

DESERT STORM provides an example of interdicting the imaging cycle at the dissemination point. During DESERT STORM, sensitive movements of the coalition forces were collected, transmitted, and processed by SPOT. However, due to U.S. diplomatic pressure, these images were not forwarded to Iraq or any nation sympathetic to Iraq. Therefore, "diplomatic pressure" is commonly mentioned as a solution to the commercial satellite imagery problem.[6]

Evaluation Criteria

Having established a means to classify different solutions to the issue of denying commercial satellite imagery, the proposed solutions are then evaluated against the major criteria of technical, operational, legal, and political feasibility. These criteria are derived from the secondary research questions, discussed in chapter 1, that support the primary research question. The following questions and weights determine the value of each of the four major criteria listed in Table 2:

Technical

A. Does the U.S. currently possess a system or mechanism to accomplish a solution of this type? (4) (i.e., a "Yes" answer to this question yields a score of "4" in the table.)

B. If not, has the technology to build such a system or methodology been demonstrated? (3) (i.e., a "No" to the first question, but a "Yes" to this question yields a score of "3" in the table.)

C. If not, have key subsystems or portions of the methodology been demonstrated? (2)

D. If not, is the technology methodology feasible in the near future? (1)

Only one of the above four scores can count in the final assessment of the technical criterion.

Operational

A. Does this system or methodology deny all of the sources of information an adversary needs or enough of them to make a difference in their decision making? (2)

B. Does this system or methodology deny the information over a sufficient length of time to be militarily significant? (1)

C. Can this system or methodology be maintained over time? (1)

Each of the questions supporting the operational criterion is independent. Question A can receive a partial score of 1 for solutions that that are effective against only a portion of the threat imaging systems.

Legal

A. Is the proposed solution consistent with all U.S. domestic law (such as the "Captain Midnight" law banning interference with all commercial satellite communications)? (2)

B. Is the proposed solution consistent with accepted international law (such as the Outer Space Treaty of 1967)? (1)

C. Is the proposed solution consistent with U.S. treaties and agreements (such as the U.S. U.S.S.R. ABM Treaty) (1)?

Each of the three questions supporting the legal criterion is independently assessed. Question A can receive a partial score of 1 for proposed solutions if the U.S. law is ambiguous on the legal status of some portion of that solution.

Political

A. Would there be international political consequences to fielding the proposed system or towards using the proposed methodology? A "No" answer scores 1. a "Yes" scores 0.

B. If the answer to question A is "Yes," could the system be fielded and operated covertly, such that employment is not attributable to the U.S.? (1)

C. Would there be negative media reaction to fielding the proposed system or methodology? A "No" answer scores 1, a "Yes" scores 0.

D. If the answer to question C is "Yes," could the system be developed and fielded covertly? (1)

E. Is the cost prohibitive? (1)

F. Does the expected military gain exceed all potential negative political consequences?(1)

Question B is linked to the answer to question A, and question D is linked to the answer to question C. Questions E and F are independently assessed. The maximum score for the political criterion, like the other criteria, has a maximum score of 4.

All proposed solutions that score 3 or higher in each of the four major criteria will be considered a potentially effective solution to the United States need to deny space-based imagery to potential adversaries. The total score is not relevant; each criterion is independently evaluated. Therefore a system that scores 4 in three categories, but only a 2 in another still fails to satisfy the above condition even though the numerical average is greater than three. Any solution that scores 4 in each major category will be considered an effective solution to the primary research problem. If no solution scores 3 or higher in every category, then the conclusion will be that the United States cannot effectively deny adversaries commercial satellite imagery. In the notional example listed in Table 2, no solution would be considered to have be completely effective and only solution #2 would be considered potentially effective in the operational denial of commercial satellite imagery.

CHAPTER 4

ANALYSIS

Chapter 2 described the threat to the United States from the proliferation of commercial satellite imaging systems. The review of the professional literature also suggested a number of potential solutions to this problem. In chapter 3, criteria for evaluating these potential solutions were defined along with a methodology for determining feasibility of the solutions according to these key criteria. In this chapter, each of the solutions is individually evaluated according to the pre-defined criteria. A summary table of the evaluations (Table 3) is presented in chapter 4.

In chapter 1, a typical imaging system was defined in terms of its principle subsystems. The evaluation in this chapter will group potential solutions according to the major subsystem affected by their action. The interaction of these subsystems is graphically depicted in Figure 1. To review this process:

1. Collect the raw data. A satellite must be in orbit above the target and have a sensor capable of imaging that target.

2. Transmit the data. The satellite must then pass the data to a ground site capable of receiving the data.

3. Process the data. The ground station then passes the data to a central processing facility to be converted into a useable product. In some cases, the ground site and the processing site are at the same location.

4. Disseminate the information. The processed data is now information and the commercial provider must transmit it by terrestrial or space links to the end users, which may include potential adversaries of the United States.

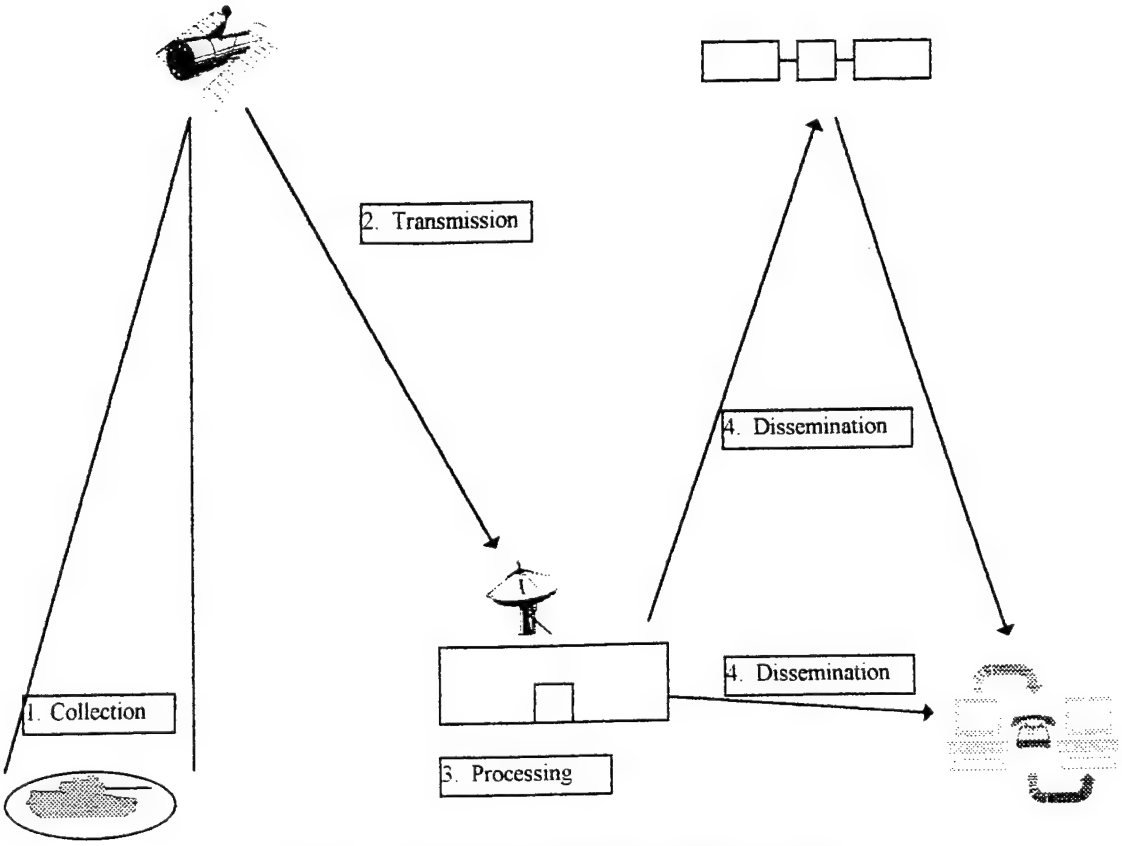

Figure 1. Commercial Satellite Imaging Process

In addition, solutions acting on the same subsystem may be distinguished by the physical mechanism they rely on to accomplish the interdiction of information.

Collection

One of the most direct methods of preventing the flow of adverse information to the wrong parties is to prevent the collection of that information in the first place. Therefore authors

who addressed this problem tended to focus on how to prevent the satellite from seeing information that the United States may not want it to see. The large number of potential methods to interdict the collection subsystem will be grouped according to the physical mechanism used to achieve the desired effect. This includes nonmateriel solutions, such as operational restrictions and cover, concealment, and deception (CCD) techniques, as well as physical solutions such as kinetic energy ASATs, nuclear radiation effects, directed energy attacks, and electromagnetic jamming of the command uplink to the satellite.

Nonmateriel Solutions

1. Passive Countermeasures. Passive countermeasures, such as limiting U.S. operations to times when an imaging system does not have the proper conditions to image, do not require any kind of technological development. The owner of every satellite is required to register its orbital characteristics according to international law.[1] In addition, USSPACECOM routinely and continuously tracks all satellites with its worldwide surveillance network. Commercial satellites orbit in completely predictable paths and every commercial satellite's physical capabilities will be known to the U.S. In fact, commercial enterprises are likely to widely advertise their capabilities to attract new business. U.S. military units routinely are advised by USSPACECOM of the times that an imaging satellite, civilian or military, will be overhead. A mechanism therefore exists to allow U.S. forces to conduct sensitive operations that the U.S. does not want an adversary to observe. Based on the technical subquestions defined in chapter 3, Passive Countermeasures receives a score of "4" for the Technical criterion.

The passive countermeasures approach involves accepting an operational restriction to conduct operations only at times when no space-based observation is possible. However, these restrictions may not be acceptable to U.S. military commanders in many situations. Although U.S. military units currently attempt to avoid conducting operations when they can be observed by

foreign systems, the number of these imaging systems is currently very small. As systems proliferate, the amount of time that operations have to be restricted increases dramatically. Certain operations cannot be effectively conducted in the increasingly shorter periods where no threat imager is overhead.

Other operations cannot be hidden from even today's commercial systems. Maneuver of large units, establishment of assembly areas, conduct of airfield activities, construction of fortifications, and movement of supplies are just a few of the types of operations that cannot be performed while conducting effective passive countermeasures against existing commercial imaging systems. As the number of imagers increases, the number of operations that can effectively employ passive countermeasures will decrease proportionately. Since some sources of information would still be available to an adversary, and the U.S. would have difficulty maintaining effective passive countermeasures over any significant length of time, the overall operational score is a 2.

Voluntarily restricting military to these times clearly poses no domestic or international legal questions and does not violate any bilateral or international agreement. This leads to a Legal score of 4, based on the Legal subquestions defined in chapter 3.

This approach is also one of the least provocative counter to commercial imaging systems possible. There are no likely domestic or international consequences to pursuing this approach and the relative cost is not prohibitive. These answers to the subquestions established for the Political criterion in chapter 3 yield a Political score of 4.

In summary, answering the questions established in the methodology for this thesis results in scores of 4, 2, 4, and 4, for the Technical, Operational, Legal and Political criteria, respectively. These results, as well as the results of all other proposed solutions will be graphically depicted in chapter 5. The meaning of this particular result is that Passive Countermeasures is not an effective

solution to the problem of denial of imagery to U.S. adversaries. The basis for this assessment is that the Operational score failed to meet the minimum threshold.

2. Cover, Concealment and Deception. Cover, concealment, and deception techniques can hide the true nature of some military units or equipment from satellites even when they are in the right position and have the right environmental conditions to image the target. These techniques can range from something as simple as covering a small piece of equipment with a camouflaged tarp, to hiding a tactical unit by generating smoke. Infrared sensors could potentially be fooled by starting fires that would mask the heat signature of certain types of equipment. In addition, the U.S. may sometimes find it advantageous to allow the imaging system to collect certain information it wants passed to the adversary to support a deception operation. The Iraqis effectively deceived the U.S. during DESERT STORM with dummy SCUD launchers and by hiding MiG fighters under bridges. They also attempted, with less success, to hide from the infrared sensors of U.S. satellites by setting fire to Kuwaiti oil wells.

The analysis of CCD techniques is similar to the analysis of passive countermeasures. Clearly the U.S. possesses the technology to implement CCD techniques, but it is also clear that certain types of units or equipment are too large or too difficult to hide. Sometimes the operational restrictions involved in attempting to conceal equipment renders the equipment operationally ineffective, such as the MiG aircraft under the bridge. In addition, it will be difficult for the U.S. commanders to know that any deception effort has worked. For example, detailed analysis of multispectral imagery was able to detect the presence of dummy SCUDs as the war went on and U.S. intelligence analysts were alerted to the deception.

Therefore, like passive countermeasures, CCD techniques receives a score of 4 for the technical, legal and political criteria, but only a 2 for the operational criterion.

3. Direct Ascent ASAT. The United States does not currently have an operational direct ascent ASAT, but has successfully demonstrated such a system against an object in space in the past. Therefore, it has a technical score of 3. Permanent destruction of the threat satellite certainly denies all information to the adversary for a substantial length of time. Since these ASATs could be produced in sufficient numbers to destroy a large portion of the potential threat imagers, the overall operational score is a 4.

While an ASAT is not inherently illegal, an ASAT attack against a third party would probably be considered a violation of international law. The permanent destruction of civilian third party satellites might be analogous to the sinking of third party shipping by Germany in World War II. While the U.S. could argue that the commercial satellite was a legitimate military target because, by international legal standards, it was illegally passing military intelligence to a U.S. adversary, the likely position of an international court would be against the U.S. Since U.S. laws and treaties do not ban ASATs, there is no domestic legal restriction to consider. However, the probable violation of international law results in an overall score of 3 for this solution.

While the cost of an operational direct ascent ASAT would not be prohibitive, the use of such a weapon would have serious international political consequences. Not only would the owning nation(s) likely consider the destruction of their satellite an act of war, but other spacefaring nations would be expected to act negatively as well given their past positions in international negotiations on the use of space. In addition, debris from the explosion of the U.S. warhead and resulting destruction of the target satellite would potentially interfere with uninvolved parties--to include U.S. civilian and military space systems. The expected media reaction to this possibility might prevent any such proposed system from ever being built in the first place. Even if such a weapon was built covertly, it could not be employed covertly and the

negative domestic and international political reaction of its employment would be a strong deterrent to its use in any but the most dire scenarios. This coupled with an unpredictable chance of fratricide and collateral damage from the debris probably mean that any military gain would not be worth the political consequences. Based on all of the above factors, the political score for this approach is a 1.

4. Co-orbital ASAT. A kinetic energy ASAT that relies on co-orbital interception of the target has many of the same advantages and disadvantages of the direct ascent ASAT system already analyzed. Although the U.S. has not tested a co-orbital ASAT, the Russians have tested it numerous times with acceptable reliability. Since the system is less technologically complex than the U.S. ASATs previously tested, it is reasonable to assume that the U.S. could develop such a system in a relatively short period of time. Therefore, the technical score is also a 3.

The operational and legal arguments remain the same, so the scores for those two criteria are 4 and 2 respectively. A co-orbital ASAT would be cheaper than a direct ascent weapon, but would be less reliable. Since its kill mechanism relies on intentionally creating a large amount of orbital debris, the fratricide, collateral damage and attendant political consequences of that debris are even more severe. Therefore the political criterion also receives a score of 1.

5. Antiballistic Missiles. Kinetic kill ABMs can potentially double as kinetic energy ASATs. Although the U.S. does not currently possess an operational ABM, it has proven the technology with previous R&D programs like ERIS in the past. As discussed in chapter 2, LEO satellites are technically less demanding targets than ICBMs. Therefore, ABMs have a technical score of 3.

Operationally, ABMs represent a permanent solution to denying an adversary access to certain imagery products, so the operational score is 4. However, the development, testing, or deployment of an ABM system is prohibited by the 1972 U.S.-U.S.S.R ABM treaty. Since the

actual use of an ABM against a satellite would also be interpreted as a violation of the 1967 Outer Space Treaty, the overall legal score for an ABM solution is only a 2.

The discussion of the political criterion is similar to that for a direct ascent ASAT, so this system receives a score of 1.

6. Ballistic Missiles. ICBMs using conventional warheads could conceivably serve as a kinetic energy ASAT. The primary advantage of this approach is that the U.S. already has operational ICBMs, so the technical score is a 4. However, ICBMs are launched from fixed sites in the United States and cannot reach all of the orbits necessary to negate all of the threat satellites, so the operational score is a 3. Use of an ICBM as a kinetic energy ASAT would still be interpreted as a violation of international law, but would otherwise be consistent with U.S. laws, so the legal score is a 3. However, all of the previous negative reactions associated with kinetic kill ASATs apply to this approach as well. The major exception is that ICBMs are already fielded for a different purpose, so there is no question about attempting to obtain public support to field the system. In addition, this method may seem more provocative in that the launch of the ICBMs might be misinterpreted as a pre-emptive nuclear strike. Therefore the political score is a 2.

7. Space-based Interceptors or Space Mines. A series of pre-deployed space-based interceptors, such as the Brilliant Pebbles portion of the canceled Strategic Defense Initiative (SDI) program could be employed against satellites more easily than ballistic missiles. Under the SDI program, several technical demonstrations supported the feasibility of such a concept, but the program was canceled before it was tested in space. Therefore the technical criterion receives a score of 2 for this approach.

A Brilliant Pebbles system could deny multiple satellites nearly simultaneously. The effects of the attacks would be permanent. Therefore, operationally this approach rates a 4. However, the same problems with international law are present, so the legal score is only a 3.

The negative political consequences of a kinetic kill attack apply to the space-based interceptor approach as well. A small number of interceptors might be placed in orbit covertly, but the vast numbers needed to guarantee the operational effectiveness against multiple commercial systems could not be hidden for long. Actual employment of the system would be unambiguous and the United States could not claim plausible deniability. In addition, the cost of building, testing and fielding a constellation of space-based interceptors would be prohibitive. The political score for this approach is 0.

8. De Facto Space Mine. Since virtually any maneuvering space object could be used as a space mine, it must be said that the U.S. has an inherent capability in space to cause a kinetic energy kill in LEO. This approach therefore has a technical score of 4. Matching the orbits of an existing impaired U.S. satellite to that of a potential satellite imager in LEO would be a complicated task. The actual maneuver would require the expenditure of a significant amount of fuel and take time to achieve the intercept. For many potential scenarios, such an interception may not even be possible. If successful, the interception would be a permanent denial of the target satellite, but the chances of success are so low as to render this an ineffective option. Therefore the overall operational score is a 2.

Given the assumption that the permanent destruction of a third party satellite would be considered a violation of international law, this approach still achieves a 3 for a legal score even though there are clearly no legal issues with placing maneuvering objects in space.

This is a more attractive solution politically as the satellites used for the attack are not placed into orbits for this purpose, but had some other nonaggressive intention. The proposal here is the use of an impaired satellite as an ad hoc ASAT, so there is no premeditation. Clearly then there will be no objection to "fielding" this system from either the international or domestic

community. The only political consequences would occur at the time of actual employment. Since this a zero cost option using existing assets, the overall political score is a 2.

Nuclear Radiation

9. Exoatmospheric nuclear explosion. A nuclear explosion in space will not only destroy a target satellite or satellites in LEO, but also physically alter the environment over a large region of space such that other imagers will be affected as they enter the region of concern. The technology to deliver a nuclear weapon close enough to have an effect is already fielded, and the U.S. has an inherent capability to conduct such an attack. Therefore the technical score is 4.

Operationally, a single nuclear burst would deny all adversary access to space-based imagery over the area of concern. Therefore the operational score is 4.

A nuclear explosion in space violates virtually every principle of space law, both legal and domestic. In addition, it violates specifics bilateral and multilateral agreements the U.S. has signed since the very beginning of space travel. The legal score is 0.

Since this approach relies on an existing system already fielded for another purpose, there are no cost of fielding issues. However, the international consequences of using such a weapon would be serious. The exact effects of the attack cannot be accurately predicted, but it is certain that many uninvolved satellites will be destroyed, damaged, or disrupted in addition to the targets. Environmental effects would linger for an unpredictable amount of time and affect a large volume of space. The launch of a nuclear weapon is probably the most provocative option imaginable. The political score is 2.

10. Nuclear-tipped ABM. An ABM, such as the former Soviet Galosh, with a very small nuclear warhead, could be used to reliably destroy a target satellite with far less collateral effects than the explosion of an ICBM in space. The United States does not possess such a system, but could easily develop this capability, so the technical score is 3.

Operationally, this approach could still permanently deny imagery to the adversary, however, more than one attack might be necessary. Since multiple attacks have been demonstrated by the former Soviets, this should not be considered a limiting factor. Therefore the overall operational score is still a 4.

Despite the smaller size of the warhead, the basic legal arguments against this proposal remain unchanged, so the legal score is still 0.

Although the fratricide and collateral damage caused by this weapon would be reduced, it would still be unacceptably high from a domestic and international viewpoint, and the act of destroying a third party satellite would still result in negative political consequences. Negative media reaction would probably prevent any system of this type from ever being built in the United States, although not for cost reasons. The political score for this approach is a 1.

11. X-Ray Laser. An X-ray laser is a device that harnesses the power of a small nuclear explosion and can produce a highly directional lethal attack. A single space-based device could fire many times and be effective at long ranges. Operationally such a system is rated as a 4.

Although the DoD conducted some R&D experiments of the components of an x-ray laser in the 1980s, it would take a significant effort to make a device like this practical. Preliminary efforts do support the technical feasibility of a device provided the proper resources. The technical score is a 1.

The fielding of an x-ray laser would be consistent with U.S. domestic law, but the employment of this weapon would likely be considered a violation of international law. In addition, there would be legal arguments that this weapon violates the Limited Test Ban treaty, even though the nuclear explosion used to power the laser is small and controlled. The legal score is a 2. Developing an X-Ray laser would be extremely expensive and could not be employed covertly. Negative media and international reaction would make it difficult to field a system and

the military gain would not normally be worth the consequences resulting from an attack. The political score is 0.

Directed Energy Weapons

12. High-powered laser--Destruct. A large, high-powered laser, like the MIRACL laser in New Mexico or the Sary Shagan laser complex in Russia, could potentially destroy satellites in LEO, without causing fratricide or collateral damage. Although the U.S. does not have an operational system, the MIRACL experiments demonstrate the feasibility of such a system. The technical score is 3.

A sufficiently powerful laser could destroy the imaging sensor of threat satellites as they orbited over the laser facility in the U.S. The satellite would continue to orbit, possibly operating other payloads, but would not be able to image targets of concern to the U.S. Since virtually all LEO satellites would pass over the site in the space of two days, this represents an operationally effective solution to problem of space-based imagery. The operational score is a 4.

The fielding of this system would not violate any law, but the actual destruction of a major payload on a commercial third-party satellite would probably be considered a violation of international law just as destruction of the entire satellite would be. The legal score is a 3.

While the use of the high-powered laser to destroy a component of a satellite would not cause the fratricide and collateral damage of kinetic energy approaches, the likely international reaction to an attack would still be serious. The cost of building a laser powerful enough to encompass all the LEO targets would likely be prohibitive. The military gain achieved by the selective disablement of threat sensors, might be considered worth the negative political consequences. A high-powered laser could be built covertly and could be employed against one or two targets while maintaining plausible deniability. The political score is a 2.

13. High Power Laser--Disrupt/Degrade. According to the United Nations Institute for Disarmament Research, the Army's MIRACL laser is not powerful enough to destroy typical commercial imaging satellites, but is powerful enough to interfere with them or possibly degrade their performance over time.[2] Since this attack mode would use an existing capability, this option will be examined as separate and distinct from the "hard-kill" laser attack previously discussed. As an existing piece of hardware could be converted to a weapon in a relatively short time, the technical score for this system is a 4, instead of a 3 for the "hard-kill" attack mode that would required further development.

Operationally, a high-powered, ground-based laser could engage all of the targets of interest and could selectively disrupt or degrade these targets over time. Therefore the operational score is a 4.

While the use of a high-powered laser to degrade or disrupt commercial satellites would not violate U.S. laws, it would most likely still be considered a violation of international law, despite the more surgical nature of the attack. The legal score is a 3.

In a 3 March 1996 Defense News article, Congressional policy analyst Marcia Smith was noted a major shift in congressional reaction to ASAT testing. The 1997 defense budget no longer includes the previous prohibition on testing ground-based lasers against objects in space. Congress also granted $30 million for future development of this technology, even though the Air Force specifically mentioned commercial imaging systems as a potential target.[3] There was little media reaction to this news, and only one senator Sen Tom Harkin (Democrat-Iowa) objected.[4] Clearly the cost of this system is not prohibitive, since it was funded in an otherwise serious defense drawdown. International reaction the actual employment of this system would still be negative, but the use of the laser from our own territory, allows potentially covert attacks. On a small scale, the United States might be able to retain plausible deniability while denying key

information to the adversary. Used on a larger scale, the attacks would be attributable to the United States, but might still be considered worth the negative international political consequences. The overall political score is a 3.

14. Space-based lasers. Placing lasers in space offers several technical advantages because the power requirements would be far smaller, and there is little atmosphere to compensate for. However, the space environment is hazardous and any space-based system is likely to be technically complex. Key components of a space-based laser system have been satisfactorily tested, but the development of an operational prototype would take many years even if the decision was made to pursue this option. The technical score is a 2.

A space-based laser system would offer many operational advantages. A constellation of small satellites could provide worldwide coverage and allow the United States to selectively deny any satellite imager at will. The operational score is a 4.

Since a space-based laser is not a weapon of mass destruction, the United States could argue that deployment of this weapon system is within the definition of international law. Other countries would likely argue successfully that the actual use of this weapon to destroy a third party was still an illegal act. In addition, a broad interpretation of the U.S.-U.S.S.R. ABM treaty might classify this system as an ABM weapon, since it would have an inherent capability against ballistic missiles as well. Therefore deployment, testing or employment of this system would violate a ratified international treaty. Although the United States could present a case that the interpretation of these two objections is questionable, it would probably not prevail. Therefore the legal score is a 2.

International reaction to the deployment of a space-based laser constellation would be extremely negative. However, this system could be deployed and probably even employed covertly. Domestic media reaction to previous proposals has been mixed, but the chief objection

would be the perceived cost to do the research, development, testing, and fielding of this system. The military value gained from employment probably outweigh any negative political consequence. The overall political score is a 3.

15. Airborne Laser. All of the subsystems for an airborne high-powered laser have been successfully tested, but there is no current operational system. The technical score is a 3.

An airborne laser system would provide operational flexibility by being a "dual-use" system against theater ballistic missiles (TBMs) or in denying satellite imagery over the AOR. The ABL could be used in a lethal destruct mode or to simply blind the satellite's imager at the key time. Multiple platforms would be required to provide continuous coverage, but can be justified for the TBM mission alone. Operationally, several ABLs could deny all satellite imagery to an adversary through either temporary or permanent effects. The operational score is a 4.

Used in a nondestructive mode, the use of a laser to temporarily blind a satellite should not be considered a violation of international law. However, this concept has never been specifically addressed. If the attack hides key military information from the satellite without damaging the satellite, then the United States could make a case that this is just another form of camouflage. Using a laser to flash the satellite's sensor for the critical moments it is in position to image U.S. forces is analogous to setting off smoke to hide our position. No U.S. domestic or international treaties place any restrictions on the use of lasers for this purpose. The legal score is a 4.

A nondestructive laser attack on a satellite would pose a dilemma for the commercial satellite operators. To protest the attack, they would have to admit that they were imaging the United States military. It is a violation of international law to image another nation without notifying that nation and providing the imagery. It is also a violation of international law to use space for other than peaceful purposes, which most countries interpret as nonmilitary. Therefore,

to accuse the United States of a belligerent act, they would first have to admit to a belligerent act themselves. This would then justify the U.S. attack. There is no negative media reaction to the development of the ABL and the cost is not prohibitive. It is unlikely that there would be any serious international consequences of selectively denying imagery on a temporary basis over critical areas of a military AOR. If there were complaints, the military advantage of providing protection to our forces probably outweighs them. The political score is a 4.

16. Low-powered Lasers. Low-powered lasers exist for other applications and could be developed readily for counterspace applications. The main technical challenges would involve correction for atmospheric losses. The Starfire Optical Range has already successfully demonstrated that these losses can be avoided through their experiments in adaptive optics.[5] The technical score is a 3.

A large number of these low-powered lasers would be needed to be operationally effective, since each could protect only a small region from being seen by a satellite imager. However, since the lasers would be relatively inexpensive and easily transportable, a relatively larger quantity could be fielded. The Services could use these lasers to deny critical imagery to the adversary. Each laser would be capable of repeated fire, needing only a few minutes in between shots to recycle. Therefore, they could engage multiple platforms that might pass over a given location. The overall operational score is a 4.

The previous discussion on the legal issues of momentarily blinding a sensor with a laser apply to this system, too. The use of this system should be legally defensible as a militarily necessary act that causes no damage. The legal score is a 4.

The deployment, testing and fielding of this system should be politically acceptable both domestically and internationally. The owners of the commercial satellites might object to the existence of these weapons, but their only use is to hide objects from images that the satellite

operators are not supposed to take in the first place. This system has an additional advantage in that it is many times less powerful than the threshold power needed to damage the sensor. Therefore, it is a relatively unprovocative method of denying imagery at the point of collection. It should be a low cost solution with little technical risk. The overall political score is a 4.

17. High-Power Microwaves. HPMs can disrupt, or degrade satellites through interference with their sensitive electronics. Considerable R&D work has been done on HPM devices, particularly in Russia, but the United States has yet to demonstrate a feasible HPM device. Based on the HPM research to date, HPM technology offers considerable military utility in the future, but will not be readily available in the short-term. The technical score is a 1.

Operationally, an HPM weapon would require a large fixed site. Temporary denial would have little operational utility since the imager would not be over the AOR the United States would want to deny to the adversary. Although HPMs theoretically can achieve effects ranging from disruption to destruction, these effects are not readily scaleable. Therefore operational utility is questionable for a majority of targets in likely scenarios. The effects may not last for a significant amount of time, or the target satellite may accidentally be destroyed. The operational score is a 1.

HPM attacks would suffer the same legal consequences as a kinetic energy ASAT, if they resulted in destruction of the commercial satellite. International treaties and domestic U.S. laws do not address HPMs. Therefore the overall legal score is a 3.

An HPM weapon could probably be built for an affordable cost, and may not encounter any significant domestic opposition. The actual employment of the weapon would most likely not be covert, and negative international political consequences will most likely result from a successful destructive attack. However, a successful destructive attack may well be worth the negative consequences, if that was the intended result. This yields an overall political score of 3.

18. Jamming the Uplink. All commercial satellites are tasked from the ground. If this signal is jammed, the satellite cannot be ordered to take images until it comes into view of another ground station. Technically, jamming requires being able to transmit on the same frequency, but with higher power, within the satellites communications path. Since the United States will not know in advance which specific imager it needs to deny, an uplink jammer must be capable of operating at different frequencies and in different geographic areas. Although the United States does not have an operational uplink jammer, it should be feasible to build one that perform the jamming mission. The technical score is a 3.

For any given commercial threat system, jamming the uplink should temporarily deny an adversary access to vital space imagery. However, for a situation where the United States is concerned with many different imaging platforms that need to be denied over a long period of time, uplink jamming is impractical. It would take too many jamming assets operating simultaneously in too many dispersed locations. The operational score is a 2.

The act of blocking a nation's command of its own satellite is illegal in most interpretations of international law. In addition, to blocking the possible hostile command to the satellite to image a U.S. target, many other nonhostile commands would be blocked as well. The health and welfare of the space asset might also be threatened by a failure to adequately receive command signals. The United States could try to make a case that jamming these commands is a temporary, nondestructive means of denial of sensitive military intelligence. However, from an international perspective, it would most likely be perceived as an illegal attack on another nation's sovereign property. The legal score is a 3.

The negative political consequences are probably acceptable, since the United States could maintain that it did not damage the targeted asset. Jamming has been frequently discussed in U.S. media and there is no significant domestic objections to the concept. The cost to build an

operationally effective suite of jammers would be high, but far less than space-based concepts. Therefore the overall political score for this option is a 4.

19. Spoofing. Spoofing is a covert method of sending false commands, rather than blocking all legitimate commands. Spoofing involves the same general technical challenges as jamming, and might even be performed with the same assets. The technical score is a 3.

Unlike jamming, spoofing requires detailed intelligence on the target system's command protocols. Unless there was advance notice of the specific system to be denied, there may not be sufficient intelligence to conduct successful spoofing. Spoofing relies on subtle, covert insertion of commands. Therefore, it cannot be used very often or the satellite's owner will become aware of the attack and perform countermeasures. Therefore, at any one time, spoofing can only deny a portion of the potential commercial satellite imagers. Although, in theory, the satellite could be sent an order that would result in its destruction, the likely use of spoofing would be for a specific denial. This could not be maintained over a long period of time. The operational score is a 2.

Legally the same issues arise as in spoofing. The primary exception is that the target may not realize that they have been attacked at all. This fact does not make the attack automatically legal. If the attack were known, it would certainly be considered illegal in the international legal forums. The legal score is a 3.

From a political perspective, this option is attractive as it does not involve expensive hardware and is extremely surgical. The covert nature of the attacks would render negative international consequences moot. The political score is a 4.

Transmission

Once a commercial satellite has collected the imagery that threatens U.S. interests, it has to pass this information down to a ground station. If this transmission is disrupted, then the

adversary will be denied the threatening information even though the third party's satellite has not been interfered with at all.

20. Downlink Jamming. An alternative to blocking the satellite's reception of commands is to block the satellite's transmission of data by putting out enough noise to prevent any information from reaching the ground. The technology to perform this task is similar to the previously discussed jammer, so the technical score is a 3.

Operationally, many of the same reservations exist for this option as existed for the uplink jammer. The primary problem is having enough jammers to interdict all of the satellite's possible transmission routes for a militarily significant period of time. In addition, the ground segment receivers may be located in a country hostile to the U.S. Getting close enough to the receiver to effectively jam its reception may not be practically if the transmission is done through a spot beam. Therefore, the operational score is a 2.

The same legal issues apply unless the United States would be capable of proving that the satellite had illegally collected military intelligence on U.S. forces. This would be very difficult to do in practice; therefore the United States would most likely be on the wrong side of international law. The legal score is a 3.

Political issues remain similar to the previous discussion, but the U.S. would have the added advantage of being able to claim that it did not attack the satellite in any way, but merely temporarily disrupted the flow of information as a defensive measure. The United States could expect criticism, but would not likely suffer serious negative consequences. The political score is a 4.

21. Disruption of Precise Navigation. As more and more commercial imaging satellites rely on GPS to provide accurate imagery, they becoming increasing vulnerable to disruption of GPS. Since the interpretation of high-resolution imagery depends on the satellite's perception of

its position, disruption of GPS would render the images as meaningless data. Disruption of GPS could take the form of deliberately degrading the signal, since the United States controls GPS. This disruption would affect many allied and civilian users as well as the commercial satellite imagers. Alternately, the U.S. could deploy space-based jammers or spoofers that would disrupt GPS in the local space environment. This would require a development program, but the feasibility of GPS jamming has already been demonstrated. The technical score for this approach is a 2.

This technique would effectively disrupt imagery taken in the region of the jamming, for those systems that rely on GPS for precise navigation. Since not all systems will have GPS, some will not be affected at all. GPS jamming would be easy to maintain for the length of time necessary to support most military operations. Since it would only be partially effective, the operational score is a 3.

There are no real legal issues with this approach because the U.S. is the sole owners of GPS and would be interfering only with their own signals. The U.S. allows other nations and commercial entities to use the service, but does not charge for the service. The U.S. has reserved the right to degrade service in times of war. The legal score is a 4.

Because the United States stipulated when it first provided GPS service that it would selectively degrade the service during times of conflict, interruption of our own satellite service should be acceptable to the international community during times of U.S. conflict. The cost of developing and deploying this kind of system would be modest and there are no anticipated domestic objections. The system could be built, tested and employed covertly allowing the National Command Authorities (NCA) flexibility in its employment. The political score is a 4.

Processing

Once the satellite has transmitted the data to a ground station, the commercial entity will process the data into a useful information product for sale. The number of options to interdict the imagery process at this point is limited to covert methods because it is unlikely that direct attacks on the terrestrial segment of a commercial third party would ever be politically acceptable.

22. Covert Cooperation. There is some instances of U.S. corporations voluntarily cooperating with the DoD to support national security interests. It is possible that some corporations would be willing to voluntarily not process potentially damaging information to the U.S. or even alter their information product to support a military deception operation. As this is a non-materiel solution, the technical score is 4.

This technique has obvious operational advantages where this cooperation can be obtained. The corporation is in the best position to know what information has been collected and processed. It can exert perfect control over what does get passed to an adversary. However, it is unlikely that this cooperation will be generally available from U.S. corporations and even less likely from non-U.S. corporations. Since the trend is increasingly towards multinational corporations deploying space assets, this is an unreliable technique for dealing with the majority of space imaging systems. The operational score is a 2.

Although this approach does not violate any international space laws, it might be considered a violation of U.S. domestic law. At least during peacetime, it could be interpreted as government participation in an attempt to commit fraud. There are no treaty issues concerning this approach. Therefore the legal score is a 3.

The primary political risk is to the cooperating commercial enterprise. The international reaction would undoubtedly hurt their competitive position. However, the chances to conduct this type of deception covertly are excellent, which should prevent the political fall-out. The cost of

implementing this approach is minimal. The DoD would likely consider the military gain to exceed the political risks. The political score is a 4.

23. Information Warfare. Another method of interdicting the processing of imagery data is to conduct Information Warfare (IW) against the location that is doing the processing. IW in this context could include computer viruses that target imagery the U.S. wants to deny, logic bombs triggered by a certain event (like the imaging of a sensitive U.S. military installation), or insertion of false data. IW techniques are still in their infancy, but are clearly within current technical capabilities, provided that the U.S. has access to the target system. The technical score is a 3.

IW depends on getting access to the commercial data automation systems involved in the processing. This access may be difficult to achieve and maintain. There may be no way to verify that the IW attack was successful even in those cases where the U.S. was able to obtain the access necessary to employ IW techniques. However, successful IW attacks provide the military with a great deal of flexibility to deny information to an adversary or even implant false information to support a deception. It is an extremely surgical technique, which selectively denies information over a significant length of time. Overall, this results in an operational score of 2.

An IW attack would be an act of war if conducted in another nation, and would violate U.S. domestic laws if conducted against a U.S. corporation. U.S. treaties do not address IW at this time. Assuming the target is a foreign corporation, the legal score is a 3.

The political ramifications of conducting an IW attack against another country are serious. However, the IW techniques are inherently covert and very difficult to trace back to the source, even when the attack is discovered. This should ensure the U.S. plausible deniability. The issue of building an IW capability is incorporated into all military doctrine and has been publicly

declared with no domestic objections. The cost of conducting these types of attacks is minimal. The political score is a 4.

Distribution

Once a commercial entity has processed data into information, it must then distribute the information to its customer. If the customer is a U.S. adversary, the U.S. may wish to try and interdict the distribution process.

Nonmateriel Solutions

24. Voluntary Cooperation. The U.S. could simply ask corporations not to provide the data when it threatens U.S. interests. There are no technical issues, so the technical score is a 4.

U.S. and foreign companies would be reluctant to voluntarily shut down a customer in most cases. Even U.S. companies would lose their competitive position if asked to do this too often, according to the CEOs of the companies that have acquired U.S. export licenses.[6] This approach would only be operationally effective in the most serious and obvious threats to the national security, and only for those companies friendly to the United States. The operational score is a 2.

Asking for voluntary cooperation does not cause any legal or political problems. The legal and political scores are both 4.

25. Presidential Ban. The President could order the cessation of transmission of imagery to U.S. adversaries. There is no technical issue, so the score is a 4.

This would effectively shut down U.S.-only companies, but would have no effect on non-U.S. corporations. Since the trend is towards multinational commercial entities, many U.S. corporations are part of a larger international body that is not bound by the decisions of the U.S.

President. This is, therefore, an unreliable way to deny information to the adversary. The operational score is a 2.

There are no legal issues since the procedure for ordering this ban was enacted as part of the legislation removing the export restrictions. The legal score is a 4. Banning the export of militarily sensitive data should not cause any serious political repercussions domestically or internationally. The political score is a 4.

26. Lawsuit. International space law prohibits the "remote sensing" of nations without notification and without providing them copies of the imagery. International law also prohibits the use of space for other than peaceful purposes and specifically holds nations financially liable for the actions of corporations acting from their soil. Therefore the U.S. could sue in international court to block the distribution of space imagery taken of military targets. As a nonmateriel solution, the technical score is a 4.

This approach would have virtually no operational effect as it would take literally years and years to reach resolution and is virtually unverifiable and unenforceable. The operational score is a 0.

Lawsuits are legal and part of accepted international politics. The cost of pursuing legal remedies is small relative to materiel solutions to the problem. The legal and political scores are both 4.

27. Diplomatic Pressure. Foreign corporations could be induced to voluntarily ban transmission of imagery to U.S. adversaries through diplomatic pressure on their host nation. This approach was successfully used in DESERT STORM. The technical score of this non-materiel solution is a 4.

The DESERT STORM example should be considered the exception rather than the rule. France had personnel at risk shoulder-to-shoulder with U.S. forces on the ground and virtually the

entire world was united against Saddam Hussein. In future conflicts, the U.S. should not expect full cooperation from foreign commercial entities who make most of their money from military-related products. The denial of imagery by this method is not easily verified, and probably cannot be sustained over a long period of time. The operational score is a 2.

There are no legal or political objections to the application of diplomatic pressure. The political and legal scores are both 4.

Physical Attack

28. Direct Attack on User Receivers. If a commercial producer of satellite imagery is to deliver its product, the end user must have some way to receive this product. Direct, physical attacks against the adversary nation, by conventional means, can destroy the capability to receive this product. Existing weapon systems would be used to conduct this attack, so the technical score is 4.

Information technology is rapidly progressing to the point that satellite imagery can be received on a variety of very small, mobile terminals. The number of these terminals are proliferating and can be placed anywhere. Satellite imagery can be passed over the internet to PCs. It is therefore becoming rapidly impractical to rely on direct attacks of receivers to deny space imagery to an adversary. The operational score is a 2.

There are no legal issues as the receivers are legitimate military targets in the context of a military conflict. The same logic applies to political issues. Both scores are a 4.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

The following Table summarizes the results of the analysis in chapter 4. The table is organized by the segment of the imagery process that the solution interdicts:

TABLE 3

DECISION MATRIX

Part I: Denial of Imagery Collection

SOLUTION	TECH	OPER	LEGAL	POLIT
Non-Materiel				
1. Passive CM	4	2	4	4
2. CCD	4	2	4	4
Kinetic Energy ASATs				
3. Direct Ascent	3	4	2	1
4. Co-orbital	3	4	2	1
5. ABMs	3	4	2	1
6. Ballistic Missiles	4	3	3	2
7. Space Interceptors	2	4	3	0
8. *De Facto* Space Mine	4	2	3	2
Nuclear Radiation				
9. Exoatmospheric burst	4	4	0	2
10. Nuclear ABM	3	3	0	1
11. X-Ray Laser	1	4	2	0
Directed Energy				
12. High-Pwr Lsr--Destruct	3	4	3	2
13. High-Pwr Lsr--Disrupt	**4**	**4**	**3**	**3**
14. Space-based lasers	2	4	2	3
15. Airborne Laser	**3**	**4**	**4**	**4**

TABLE 3 (cont)

DECISION MATRIX

Part I: Denial of Imagery Collection

SOLUTION	TECH	OPER	LEGAL	POLIT
Directed Energy (cont)				
16. Low-Power Lasers	**3**	**4**	**4**	**4**
17. HPM	1	1	3	3
Electronic Warfare				
18. Uplink Jamming	3	2	3	4
19. Spoofing	3	2	3	4

(Part II: Denial of Imagery Dissemination)

SOLUTION	TECH	OPER	LEGAL	POLIT
20. Downlink Jamming	3	2	3	4
21. GPS signal denial	2	3	4	4

(Part III: Denial of Imagery Processing)

SOLUTION	TECH	OPER	LEGAL	POLIT
22. Covert Cooperation	4	2	3	4
23. IW	3	2	3	4

(Part IV: Denial of Imagery Distribution)

SOLUTION	TECH	OPER	LEGAL	POLIT
Nonmateriel Solutions				
24. Voluntary Cooperation	4	2	4	4
25. Presidential Ban	4	2	4	4
26. Lawsuit	4	0	4	4
27. Diplomatic Pressure	4	2	4	4
Physical Attack				
28. Direct attack on User	4	2	4	4

None of the above solutions scored 4 in each of the decision criteria. This means that the U.S. does not currently possess a completely acceptable solution to the problem of denying commercial

satellite imagery. However three of the solutions might potentially be acceptable methods to effectively deny commercial satellite imagery to an adversary. They are: (1) Disruption of a target satellite from a high-power, ground-based laser; (2) Disruption of a target satellite or temporary blinding of an imaging sensor by an ABL; and,(3) Temporary blinding of an imaging sensor by a mobile, low-power laser. These three solutions are somewhat related and all involved the use of directed energy weapons against the satellite, or some portion of that satellite. Attacking the space segment is the most reliable method of ensuring that potentially threatening information does not reach a U.S. adversary, because it prevents the collection of that imagery in the first place.

Lasers are proven technology and possess several significant military advantages. They are precise weapons that can deliver literally "surgical" attacks. They are accurate even over extreme distances. A laser from the Starfire Optical Range, successfully hit the Galileo spacecraft on its way to Jupiter.[1] Laser emissions are very difficult to detect and are completely scaleable. This offers the National Command Authorities (NCA) a wide range of attack options--from low power jamming of sensors to overt or covert destruction of the target asset. Lasers attack with the speed of light, and new advances in adaptive optics have made distance the only limiting factor affecting the power they deliver to the target. Laser weapons do not leave space debris like kinetic energy attacks or large electronic signatures like EW, nuclear, or HPM attacks.

The primary drawbacks to laser attacks on commercial space targets are legal and political concerns. Other nations would almost certainly perceive a laser attack as an illegal act, if they could detect that it had occurred. Destruction or damage of a civilian third party asset would likely tilt world opinion against the U.S. unless the military necessity was obvious to other nations. The potential to covertly employ these weapons mitigates these concerns for some

situations. Non-destructive attacks may also reduce the potential international consequences for more general situations.

The domestic climate appears to support development of this class of weapons. A March 1996 Scientific Advisory Board (SAB) study advocated that an operational high-powered laser be built in the next decade.[2] Congress has cooperated with this recommendation by allocating funds to this effort in its 1997 budget and dropping its previous ban on testing the MIRACL ground-based laser against objects in space.[3] The SAB report specifically mentioned applications against commercial satellites without creating any kind of public backlash. Indeed, the use of laser devices against commercial satellites would be completely consistent with all U.S. domestic laws, national policies, and U.S. interpretations of treaties and international law. Its use would be subject only to the same restrictions placed on any military force. The Rule of Proportionality would require that the U.S. achieve a military gain sufficient to justify the potential interference with civilian property and would be obligated to reduce the damage inflicted to the lowest level necessary to perform the mission.

The U.S. has an existing R&D facility at White Sands, New Mexico, that is capable of performing non-destructive attacks against some LEO satellites. The technology is mature enough to develop this R&D facility into an operational weapon system. The primary limitation of this hypothetical weapon system would be its fixed location in the U.S., thus limiting its attack to those targets overhead.

However, high-power lasers can be mounted on airborne platforms and flown to the geographic location required. This is a particularly attractive option as the aircraft could simultaneously perform its primary mission of countering adversary TBMs. The technology to integrate a high-powered laser into an airborne platform has been demonstrated in field tests conducted over a 20 year period. An operational system could be delivered by the year 2001.

A large quantity of small tactical lasers could be procured and issued to Army maneuver units, capital Navy ships and any other key military units that require protection from enemy reconnaissance. The lasers have already been built and tested; further development would be required to make these lasers mobile and still accurately track and engage satellites. The totally nondestructive nature of this system makes this approach attractive as an openly acknowledged solution to imagery denial. Electronic deception is routinely done to hide the location and disposition of ships or aircraft, even in peacetime. Lasers are nothing more than energy emitted in a different part of the electromagnetic spectrum. Laser jamming should be as commonly accepted in military units as EW is today. The United States has an obvious right to hide from sensors that are not supposed to be looking in the first place. Only the offending information is blocked, so there is little political or legal downside to this solution.

At least ten solutions were acceptable from an technical, legal and political perspective, but fell short in meeting operational requirements for an effective denial system. Particularly non-materiel solutions, like diplomatic pressure, commercial cooperation, CCD techniques, or passive countermeasures, were capable of denying some types of information in certain situations. These solutions are the least provocative and most likely to be used if mission performance could be assured. However, this thesis has rejected them because they are not *generally* effective. This does not imply that they should not continue to be used in those special situations where they can be effective.

Thesis Question

Can the United States deny the use of commercial imagery to adversaries during times of hostilities? Currently the U.S. could deny some types of imagery in special situations, but does not have a system or methodology to deny key information from reaching a typical adversary. The United States could potentially develop one or more of three proposed laser systems into a

near-term solution to the general problem. This type of solution would be technically feasible, legal and politically acceptable, and operationally effective against the general class of commercial satellite imagers. In conjunction to this hardware development, a family of non-materiel solutions could deny some portion of the threat information and might be considered less provocative.

Recommendations for Further Inquiry

The United States should pursue directed energy weapons for applications against space objects. Further research needs to define the appropriate operational force structure, rules of engagement, tactics, and required resources for an effective system(s). Integration of this new class of weapons into the current command and control structure of the Services is another area that needs better definition.

This thesis rejected denial of navigation signals to commercial satellites as a potential solution. The reason for this rejection was the technical immaturity of the concept. Further research should explore the technical feasibility of this unexplored method, as it offers a completely effective and acceptable method to disrupt satellite imagery without actually attacking the threat satellite.

Information warfare is still in its infancy, but has considerable potential for applications against this class of targets. IW offers the NCA great flexibility in situations where it may be impractical to attack the collection system. For example, U.S. forces could be using the same sensor platform as the adversary. The U.S. currently accounts for over 80 percent of the commercial imagery business, and this is actually a likely situation. IW allows the denial of the information to the adversary, while allowing the U.S. the same information. While much has been written on the inevitability of IW, more scholarly work needs to be done on how IW could be employed. How could the U.S. obtain the level of access to a commercial enterprise in peacetime,

so that it could ensure the viability of IW attacks during times of hostilities? How would the United States verify that this type of attack succeeded? What would be the legal status of the personnel that make the attack? These and other questions would have to be answered before the United States could rely on IW to solve this particular problem.

ENDNOTES

Chapter 1

[1] "Efforts Call for Broader Imagery Access," The Washington Post, 20 Nov 1994: A-2.

[2] H. Norman Schwarzkopf, Press Conference, produced by CNN, 90 minutes, Russo, Feb 1991, videocassette.

[3] Peter S. Kindsvatter, "VII Corps in the Gulf," Military Review 23 (January 1992): 2. Excerpt reprinted in US Army Command and General Staff College, C310 Advance Book, Ft Leavenworth: USACGSC, 1991: 7.

[4] Congress, Joint Hearing, Committee on Science, Space, and Technology and the Permanent Select Committee on Intelligence, Commercial Remote Sensing in the Post-Cold War Era, 100th Cong., 1st sess., 1990, Committee Print: 91.

[5] Congress, Joint Hearing, Committee on Science, Space, and Technology and the Permanent Select Committee on Intelligence, Commercial Remote Sensing in the Post-Cold War Era, 103rd Cong., 2nd sess., 1994, Committee Print: 124.

[6] Andrew Wilson, "Spies in the sky for hire: Russian military reconnaissance satellites on commercial missions," 22 Jane's Defence Weekly (17 Sep 94): 33.

[7] Cong., Joint, Science, Space, and Technology and Intelligence, Commercial Remote Sensing, Committee Print 124.

[8] U.S. Army, Space Reference Text (Ft Leavenworth, KS: U.S. Army Space Institute, July 1993), F-1 - F-9.

[9] Sun Tzu, The Art of War, (London: Oxford University Press, 1963), 106.

[10] U.S. Army, FM 100-5, Operations (Washington DC: Department of the Army, 1993), 6-10-6-23.

[11] U.S. Air Force, AFM 1-1, Basic Aerospace Doctrine of the United States Air Force (Washington: Department of the Air Force, 1992), 103-115.

[12] U.S. Air Force, Draft Revision to AFM 1-1, Basic Aerospace Doctrine of the United States Air Force (Washington DC: Department of the Air Force, Jul 1995), 14-25.

Chapter 2

[1] Congress, Joint Hearing, Committee on Science, Space, and Technology and the Permanent Select Committee on Intelligence, Commercial Remote Sensing in the Post-Cold War Era, 103rd Cong., 2nd sess., 1994, Committee Print 124.

[2] Ibid.

[3] Gregory J. Bowens. "Intelligence: Senators Warn Spymasters to get down to Business," Congressional Quarterly Weekly Report 51 (1993): 3212.

[4] James G. Lee, "Counterspace Operations for Information Dominance" (Thesis: School of Advanced Airpower Studies, Maxwell Air Force Base, AL, October 1994), 15.

[5] Hugh De Santis, "Commercial Observation Satellites and their Military Implications: A Speculative Assessment," Washington Quarterly 12 (Summer 1989): 185.

[6] Andrew Wilson, "Spies in the sky for hire: Russian military reconnaissance satellites on commercial missions," Jane's Defence Weekly 22 (17 Sep 94): 33.

[7] Donald A. Meyer. "Space Countersurveillance: A Requisite for Theater Defense Planning." (Individual Study Project, U.S. Naval War College, May 1993), 6-12.

[8] Lawrence D. Hunt and Jeffrey L. Miller, "Survey of United States Commercial Satellites in Geosynchronous Earth Orbit," (Master's Thesis, Naval Postgraduate School, September, 1994), 257.

[9] Edwin C. Swedberg, The Effect on Operational and Tactical Surprise by U.S. Military Forces due to the Proliferation of Unclassified Satellite Imaging Systems (Thesis, Command and General Staff College, Ft. Leavenworth, KS, 1995), 18-35.

[10] Memo, Michael Zehner to Air Force General Counsel, General Overview of Space Law Relevant to National Security Activities, May 1995, Washington, D.C., 9.

[11] Ibid., 10.

[12] Ibid., 11.

[13] U.S. Army, Space Reference Text (Ft. Leavenworth, KS: U.S. Army Space Institute, July 1993), 3-2.

[14] Ibid., 3-2 - 3-3.

[15] Zehner, Memo, 12.

[16] Ibid.

[17] James T. Hackett and Robin Ranger, "Proliferating Satellites Drive U.S. ASAT Need," Signal 44 (May 1990): 155.

[18] US Air Force, AFDD 4, Space Operations Doctrine. (Washington, DC: Department of the Air Force, 1993) 2.

[19] Pat Cooper and Jason Glashow, "New U.S. Army Tenet Focuses on Info Control," Defense News 20 (December 1995): 12.

[20] Nandasiri Jasentuliyana, Space Law: Development and Scope (London: International Institute of Space Law, 1992), 46.

[21] Harry Feder, "The Sky's the Limit? Evaluating the International Law of Remote Sensing," International Law and Politics 23:599 (Winter 1991): 605.

[22] United Nations Institute for Disarmament Research, Satellite Warfare: A Challenge for the International Community, (Geneva: French Institute for International Relations, 1987) 21.

[23] Jasentuliyana, Space Law: Development and Scope, 145-146.

[24] Ibid.

[25] United States v. List et al., in "Trials of War Criminals before the Nuremberg Military Tribunals", vol. XI, (Washington D.C.: US Government Printing Office, 1950), 1253.

[26] Feder, "The Sky's the Limit? Evaluating the International Law of Remote Sensing," 605.

[27] Zehner, 3.

[28] Bin Cheng, "The Commercial Development of Space: The Need for New Treaties," Journal of Space Law, 19 (1991): 28.

[29] Hackett, "Proliferating Satellites Drive U.S. ASAT Need," 155.

[30] Hunt, "Survey of United States Commercial Satellites in Geosynchronous Earth Orbit," 260.

[31] Feder, "The Sky's the Limit? Evaluating the International Law of Remote Sensing," 607.

[32] Cheng, "The Commercial Development of Space: The Need for New Treaties," 36.

[33] Zehner, 4. [34] Ibid., 8. [35] Ibid., 9.

[36] Feder, "The Sky's the Limit? Evaluating the International Law of Remote Sensing," 599-601.

[37] Ibid., 617. [38] Ibid., 615. [39] Ibid., 616. [40] Zehner, 9. [41] Ibid., 10.

[42] United Nations Institute for Disarmament Research, Satellite Warfare: A Challenge for the International Community, 37.

[43] Edwin C. Swedberg, The Effect on Operational and Tactical Surprise by U.S. Military Forces due to the Proliferation of Unclassified Satellite Imaging Systems, 73.

[44] Cong., Joint, Space, Science and Technology, Intelligence, Hearing, 124.

[45] U.S. Air Force, Space Operations Doctrine, 14.

[46] Ibid.

[47] Cooper, Defense News, 12.

[48] United Nations Institute for Disarmament Research, Satellite Warfare: A Challenge for the International Community, 16.

[49] Hackett, "Proliferating Satellites Drive U.S. ASAT Need," 158.

[50] United Nations Institute for Disarmament Research, Satellite Warfare: A Challenge for the International Community, 15-16.

[51] Dana J. Johnson, Trends in Space Control Capabilities and Ballistic Missile Threats: Implications for ASAT Arms Control, (Santa Monica, CA: the RAND Corporation, March 1990), 10.

[52] J. Sullivan et. al., Limitations on High Altitude Anti-Satellite Weapons (U), Report No. JSR-86-900 (McLean, VA: The MITRE Corporation), 13.

[53] Ibid.

[54] United Nations Institute for Disarmament Research, Satellite Warfare: A Challenge for the International Community, 15.

[55] Jasentuliyana, Space Law: Development and Scope, 145-146.

[56] Hackett, "Proliferating Satellites Drive U.S. ASAT Need," 158.

[57] Lee, Counterspace Operations for Information Dominance, 31.

[58] United Nations Institute for Disarmament Research, Satellite Warfare: A Challenge for the International Community, 12.

[59] Johnson, Trends in Space Control Capabilities and Ballistic Missile Threats: Implications for ASAT Arms Control, 11.

[60] Phillips Laboratory, "Airborne Laser Concept Definition," (Briefing to Air Force Chief of Staff, Pentagon, 1994), 4.

[61] Ibid., 5.

[62] Franklin Feber, "Out-of-Band Laser Jamming of Optical Sensors" (Unsolicited Proposal, San Diego: JAYCOR, March 1994), 1.

[63] Hackett, "Proliferating Satellites Drive U.S. ASAT Need," 158.

[64] Lee, Counterspace Operations for Information Dominance, 31-32.

[65] United Nations Institute for Disarmament Research, Satellite Warfare: A Challenge for the International Community, 12.

[66] Lee, Counterspace Operations for Information Dominance, 32.

[67] United Nations Institute for Disarmament Research, Satellite Warfare: A Challenge for the International Community, 12.

[68] U.S. Air Force, Space Operations Doctrine, 15.

[69] Lee, Counterspace Operations for Information Dominance, 32.

[70] Donald A. Meyer. "Space Countersurveillance: A Requisite for Theater Defense Planning," 14.

[71] Joseph W. Cook III, et al. "Nonlethal Weapons: Technologies, Legalities, and Potential Policies," (Research Paper, Air University, 1996) 9.

[72] Laszlo Szentpeteri, "PRARE--A New, High-Precision, Microwave Satellite Tracking System for Earth Science Applications," (Proposal, Foreign Aerospace Science and Technology Center, December 1993) 1.

Chapter 3

[1] U.S. Army, ST 25-1, Resource Planning and Allocation (Ft Leavenworth KS: Command and General Staff College, 1996), 2-9.

[2] Edwin C. Swedberg, The Effect on Operational and Tactical Surprise by U.S. Military Forces due to the Proliferation of Unclassified Satellite Imaging Systems, thesis Paper, (Command and General Staff College, Ft Leavenworth, KS), 73.

[3] James G. Lee, Counterspace Operations for Information Dominance, Thesis Paper (Maxwell Air Force Base, AL: School of Advanced Airpower Studies, October 1994), 31.

[4] Joseph W. Cook III, et al. "Nonlethal Weapons: Technologies, Legalities, and Potential Policies," (Research Paper, Air University, 1996) 9.

[5] SPOT Image Corporation (1996, April). SPOT Home Page [9 paragraphs]. Hostname: http://www.spot.com/

[6] Swedberg, The Effect on Operational and Tactical Surprise by U.S. Military Forces due to the Proliferation of Unclassified Satellite Imaging Systems, 72-73.

Chapter 4

[1] Nandasiri Jasentuliyana, Space Law: Development and Scope (London: International Institute of Space Law, 1992), 46.

[2] United Nations Institute for Disarmament Research, Satellite Warfare: A Challenge for the International Community, (Geneva: French Institute for International Relations, 1987) 21.

[3] Pat Cooper, "AF Panel Projects Antisatellite Laser in Future Warfare," Defense News 21 (March 1996): 27.

[4] Ibid.

[5] Phillips Laboratory, GBL Technology Program Spinoffs and Technology Applications (Albuquerque: Department of the Air Force, 1995), 19-20.

[6] Congress, Joint Hearing, Committee on Science, Space, and Technology and the Permanent Select Committee on Intelligence, Commercial Remote Sensing in the Post-Cold War Era, 103rd Cong., 2nd sess., 1994, Committee Print: 124.

Chapter 5

[1] Phillips Laboratory, GBL Technology Program Spinoffs and Technology Applications (Albuquerque: Department of the Air Force, 1995), 26.

[2] Pat Cooper, "AF Panel Projects Antisatellite Laser in Future Warfare," Defense News 21 (March 1996): 4.

[3] Ibid., 27.

LIST OF ABBREVIATIONS

ABL	Airborne Laser
ABM	AntiBallistic Missile
AFM	Air Force Manual
AOR	Area of Responsibility
ASAT	AntiSatellite
CCD	Cover, Concealment, and Deception
CENTCOM	Central Command
CEO	Chief Executive Officer
CIA	Central Intelligence Agency
COIL	Chemical Oxygen Iodine Laser
COPUOS	Committee on Peaceful Uses of Outer Space
DEW	Directed Energy Weapon
DOD	Department of Defense
EMP	Electromagnetic Pulse
ERIS	Exoatmospheric Reentry Interceptor System
EW	Electronic Warfare
GPS	Global Positioning System
HF	Hydrogen-Fluoride
HPM	High Powered Microwave
ICBM	Intercontinental Ballistic Missile

INMARSAT	International Maritime Satellite Corporation
INTELSAT	International Telecommunication Satellite Organization
IW	Information Warfare
JFC	Joint Force Commander
km	kilometer
KTO	Kuwaiti Theater of Operations
LEO	Low Earth Orbit
MIRACL	Mid-Range Advanced Chemical Laser
MRV	Miniature Homing Vehicle
Mw	Megawatt
NCA	National Command Authority
NSD	National Security Directive
NSDD	National Security Decision Directive
NSDM	National Security Decision Memorandum
OODA	Observe-Orient-Decide-Act
PC	Personal Computer
PD	Presidential Directive
R&D	Research and Development
ROW	Rest of World
SAB	Scientific Advisory Board
SDI	Strategic Defense Initiative
SPOT	*Satellite pour l'observation de la terra*
SRAM	Short-Range Attack Missile
TBM	Theater Ballistic Missile

TTC	Tracking, Telemetry, and Control
UN	United Nations
US	United States
USSR	Union of Soviet Socialist Republics

GLOSSARY

ASAT. An antisatellite weapon. Any system designed to destroy satellites. For purposes of this thesis, use is limited to so called "hard-kill" systems where permanent loss of utility is I inflicted on a particular asset. However, this term will be used broadly enough to encompass different technologies that achieve this result.

Bandwidth. The width of a given frequency band in Hertz. The bandwidth is determined by subtracting the lowest frequency in the operating spectrum from the highest. In general, an asset with greater bandwidth has greater capacity. Transmitters cannot pass certain types of information if the bandwidth is too narrow.

Bus. Everything on a satellite except the payload(s). The bus includes the structural frame, power, attitude control, thermal management systems and tracking, telemetry and control subsystems. The bus supports the payload, but the payload performs the mission of the satellite.

Collateral Damage. Damage inflicted unintentionally on people or objects other than the target. The Law of Armed Conflict requires military planners to limit the collateral damage inflicted on noncombatants to the minimum necessary.

Constellation. A system of like satellites. Constellations are usually designed to provided increased coverage and redundancy for essential mission functions.

Control Segment. One of three components of any space system. The control segment provides for stationkeeping, orbital changes, attitude and stabilization changes, and other general maintenance activities.

Crosslink. A satellite-to-satellite communications link. Crosslinks allow control of a satellite not in view of a control segment.

Directed Energy. Concentrated energy in a tight beam, like a laser.

Exoatmospheric. Actions taken beyond the atmosphere. There is no clear definition of where the atmosphere ends and where space begins, but generally anything above 90 miles would be considered exoatmospheric.

Fratricide. Damage unintentionally done to friendly people or objects, usually referring to friendly combatants. All operations must attempt to reduce the chance of fratricide to lowest practical level.

Geostationary Orbit. A satellite that has a period of one day and orbits the equator. To a ground-based observer, the satellite will appear to remain in the same fixed location in the sky. Low Earth Orbit (LEO). A satellite rapidly orbiting the Earth at a low altitude (approximately 200-1500 kilometers (km)) is said to be in LEO. Almost all satellite imagery is collected by satellites in LEO.

High-resolution Imagery. Very high quality images taken by a sensor. There is no specific boundary that distinguishes high and medium resolution, but one meter resolution is generally considered high resolution in the context of satellite imagery. Resolution refers to the smallest size object that can be defined in a picture element.

Information Warfare. Warfare involving the interdiction of timely accurate information to an adversary. In the broadest sense, information warfare could include virtually every type of conventional warfare. However, the term usually refers to nonlethal interference with automated data processing or telecommunications equipment by unconventional attacks. Examples would include viruses, logic bombs, worms, and some types of electronic warfare.

Multispectral. A means of subdividing the spectrum into smaller bandwidths. Adding or subtracting these subdivisions can be useful in terrain or target analysis.

Operational Denial. Interference with an asset that significantly denies that asset to an adversary during military operations. The denial may take the form of degradation, disruption, or destruction and have temporary or permanent effects. Successful operational denial has an impact on the adversary's military capability by preventing the use of the targeted asset at a critical time during military operations.

Particle Beam. Streams of subatomic particles that are accelerated to high fractions of the speed of light and formed into a tight beam that does not diverge.

Payload. The portion of a satellite that performs the satellite's primary mission. A payload must be supported by a bus. There can be multiple payloads on a satellite.

Plausible Deniability. The ability to conduct an operation without the results of the operation being necessarily attributed to the nation conducting the operation. Plausible deniability is useful in allowing the conduct of operations that would have negative political consequences in the international arena.

Remote Sensing. The act of imaging the Earth from space. The image could be collected in any part of the electromagnetic spectrum by an unmanned spacecraft.

Scintillation. Excitation of atoms into an unnatural high energy state. Scintillation occurs as the result of high powered events such as nuclear explosions. Scintillation alters the physical properties of the space environment, possibly interfering with space operations.

Space Segment. One of three components of any space system. The space segment is the portion that is physically in space.

Tracking, Telemetry and Control (TTC). Electronic remote monitoring of a satellite's functions and position in space. Used by the control segment to maintain or adjust the space segment.

Terminal Segment. The last of the three components of any space system. The Terminal segment receives space-based data, either unprocessed or processed.

BIBLIOGRAPHY

Articles and Periodicals

Bowens, Gregory J. "Intelligence: Senators Warn Spymasters to get down to Business," Congressional Quarterly Weekly Report 51 (1993): 3212.

Cheng, Bin. "The Commercial Development of Space: The Need for New Treaties," Journal of Space Law, 19 (1991): 28.

Cooper, Pat. "AF Panel Projects Antisatellite Laser in Future Warfare," Defense News 21 (March 1996): 4

Cooper, Pat and Jason Glashow. "New U.S. Army Tenet Focuses on Info Control," Defense News 20 (December 1995): 12.

"Efforts Call for Broader Imagery Access," The Washington Post 20 Nov 1994: A-2.

Feder, Harry. "The Sky's the Limit? Evaluating the International Law of Remote Sensing," International Law and Politics 23:599 (Winter 1991): 605.

Hackett, James T. and Robin Ranger. "Proliferating Satellites Drive U.S. ASAT Need," Signal 44 (May 1990): 155.

Kindsvatter, Peter S. "VII Corps in the Gulf," Military Review 23 (January 1992): 2. Excerpt reprinted in US Army Command and General Staff College, C310 Advance Book, Ft Leavenworth: USACGSC, 1991: 7.

Santis, Hugh De. "Commercial Observation Satellites and their Military Implications: A Speculative Assessment," Washington Quarterly 12 (Summer 1989): 185.

Wilson, Andrew. "Spies in the sky for hire: Russian military reconnaissance satellites on commercial missions," Jane's Defence Weekly 22 (17 Sep 94): 33.

Books

Jasentuliyana, Nandasiri. Space Law: Development and Scope (London: International Institute of Space Law, 1992).

Tzu, Sun. The Art of War, (London: Oxford University Press, 1963).

Commercial Pamphlets

Feber, Franklin. "Out-of-Band Laser Jamming of Optical Sensors" (Unsolicited Proposal, San Diego: JAYCOR, March 1994).

Johnson, Dana J. Trends in Space Control Capabilities and Ballistic Missile Threats: Implications for ASAT Arms Control, (Santa Monica, CA: the RAND Corporation, March 1990).

Sullivan., J. Limitations on High Altitude Anti-Satellite Weapons (U), Report No. JSR-86-900 (McLean, VA: The MITRE Corporation).

Internet

SPOT Image Corporation (1996, April). SPOT Home Page [9 paragraphs]. Hostname: http://www.spot.com/

Government Publications

Congress, Joint Hearing, Committee on Science, Space, and Technology and the Permanent Select Committee on Intelligence. Commercial Remote Sensing in the Post-Cold War Era, 100th Cong., 1st sess., 1990, Committee Print: 91.

_____. 103rd Cong., 2nd sess., 1994, Committee Print: 124.

Phillips Laboratory. GBL Technology Program Spinoffs and Technology Applications (Albuquerque: Department of the Air Force, 1995).

United Nations Institute for Disarmament Research. Satellite Warfare: A Challenge for the International Community, (Geneva: French Institute for International Relations, 1987).

United States v. List et al.. Trials of War Criminals before the Nuremberg Military Tribunals, vol. XI, (Washington D.C.: US Government Printing Office, 1950).

US Air Force. AFDD 4, Space Operations Doctrine. (Washington, DC: Department of the Air Force, 1993).

U.S. Air Force. AFM 1-1, Basic Aerospace Doctrine of the United States Air Force (Washington: Department of the Air Force, 1992).

U.S. Air Force, Draft Revision to AFM 1-1, Basic Aerospace Doctrine of the United States Air Force (Washington DC: Department of the Air Force, Jul 1995).

U.S. Army, FM 100-5, Operations (Washington DC: Department of the Army, 1993).

U.S. Army, Space Reference Text (Ft Leavenworth, KS: U.S. Army Space Institute, July 1993).

U.S. Army, ST 25-1, Resource Planning and Allocation (Ft Leavenworth KS: Command and General Staff College, 1996).

Memoranda and Papers

Cook, Joseph W. III. "Nonlethal Weapons: Technologies, Legalities, and Potential Policies" Research Paper, Air University, 1996.

Hunt, Lawrence D. and Jeffrey L. Miller. "Survey of United States Commercial Satellites in Geosynchronous Earth Orbit." Master's Thesis, Naval Postgraduate School, September, 1994.

Lee, James G. "Counterspace Operations for Information Dominance." Thesis: School of Advanced Airpower Studies, Maxwell Air Force Base, AL, October 1994.

Meyer, Donald A. "Space Countersurveillance: A Requisite for Theater Defense Planning." Individual Study Project, U.S. Naval War College, May 1993.

Schwarzkopf, H. Norman. Interview by international press pool, produced by CNN, 90 minutes, Russo, Feb 1991, videocassette.

Swedberg, Edwin C. "The Effect on Operational and Tactical Surprise by U.S. Military Forces due to the Proliferation of Unclassified Satellite Imaging Systems." Thesis, Command and General Staff College, Ft. Leavenworth, KS, 1995.

Szentpeteri, Laszlo. "PRARE--A New, High-Precision, Microwave Satellite Tracking System for Earth Science Applications." Proposal, Foreign Aerospace Science and Technology Center, December 1993.

Zehner, Michael. "General Overview of Space Law Relevant to National Security Activities." Memo to Air Force General Counsel, Washington, D.C.: May 1995.

INITIAL DISTRIBUTION LIST

1. Combined Arms Research Library
U.S. Army Command and General Staff College
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

2. Defense Technical Information Center
Cameron Station
Alexandria, VA, 22314

3. Air University Library
Maxwell Air Force Base
AL 36112

4. LTC Deborah D. Gregoire
Department of Joint and Combined Operations
U.S. Army Command and General Staff College
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

5. LTC James C. McNaughton
Defense Language Institute
Foreign Language Center (ATZP-MH)
Presidio of Monterey, CA 93944-5006

6. Dr Vicky LH Scherberger
U.S. Army Command and General Staff College
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

7. COL David J. Aderhold
AFSPC/DOY
Peterson AFB, CO, 80901

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 07 / Jun / 96

2. Thesis Author: MAJ Anthony J. Russo

3. Thesis Title: The Operational Denial of Commercial Space Imagery

4. Thesis Committee Members Signatures:

Deborah Gregoire

James C. McMahon

Dudley W. Schneider, PhD

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

(A) B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

Fill in limitation justification for your thesis below:

Limitation Justification Statement	Chapter/Section	Page(s)

7. MMAS Thesis Author's Signature: Anthony J. Russo

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals.)

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation--release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).